

**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**

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo <sup>(1)</sup>,

deliberando secondo la procedura legislativa ordinaria <sup>(2)</sup>,

considerando quanto segue:

- (1) Instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.
- (2) Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.
- (3) La direttiva 1999/93/CE del Parlamento europeo e del Consiglio <sup>(3)</sup> trattava le firme elettroniche senza fornire un quadro transfrontaliero e settoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego. Il presente regolamento rafforza ed estende l'acquis di tale direttiva.
- (4) La comunicazione della Commissione del 26 agosto 2010, dal titolo «Agenda digitale europea» ha individuato nella frammentazione del mercato digitale, nella mancanza di interoperabilità e nell'aumento della criminalità cibernetica i grandi ostacoli al circolo virtuoso dell'economia digitale. Nella relazione 2010 sulla cittadinanza dell'UE, intitolata «Eliminare gli ostacoli all'esercizio dei diritti dei cittadini dell'Unione», la Commissione ha ulteriormente sottolineato la necessità di risolvere i principali problemi che impediscono ai cittadini dell'Unione di godere dei vantaggi di un mercato unico digitale e di servizi digitali transfrontalieri.
- (5) Nelle conclusioni del 4 febbraio 2011 e del 23 ottobre 2011 il Consiglio europeo ha invitato la Commissione a creare un mercato unico digitale entro il 2015, a fare rapidi progressi in settori essenziali dell'economia digitale e a promuovere un mercato unico digitale pienamente integrato favorendo l'impiego transfrontaliero dei servizi online, con particolare riguardo all'agevolazione dell'identificazione e dell'autenticazione elettronica sicura.

<sup>(1)</sup> GU C 351 del 15.11.2012, pag. 73.

<sup>(2)</sup> Posizione del Parlamento europeo del 3 aprile 2014 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 23 luglio 2014.

<sup>(3)</sup> Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa a un quadro comunitario per le firme elettroniche (GU L 13 del 19.1.2000, pag. 12).

- (6) Nelle conclusioni del 27 maggio 2011, il Consiglio ha invitato la Commissione a contribuire al mercato unico digitale creando le condizioni adatte per il riconoscimento reciproco transfrontaliero di funzioni essenziali quali l'identificazione elettronica, i documenti elettronici, le firme elettroniche e i servizi elettronici di recapito, nonché per l'interoperabilità dei servizi di eGovernment in tutta l'Unione europea.
- (7) Nella risoluzione del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico <sup>(1)</sup>, il Parlamento europeo ha sottolineato l'importanza della sicurezza dei servizi elettronici, in particolare delle firme elettroniche, e della necessità di creare un'infrastruttura pubblica essenziale a livello paneuropeo ed ha invitato la Commissione ad allestire un Portale europeo delle autorità di convalida per garantire l'interoperabilità transfrontaliera delle firme elettroniche e per aumentare la sicurezza delle transazioni effettuate utilizzando Internet.
- (8) La direttiva 2006/123/CE del Parlamento europeo e del Consiglio <sup>(2)</sup> dispone che gli Stati membri creino «sportelli unici» per garantire che tutte le procedure e formalità relative all'accesso a un'attività di servizi ed al suo svolgimento possano essere facilmente espletate a distanza ed elettronicamente attraverso lo sportello unico corrispondente e con le autorità competenti. Numerosi servizi online accessibili presso gli sportelli unici richiedono l'identificazione, l'autenticazione e la firma elettroniche.
- (9) In molti casi i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri. Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica riconosciuti reciprocamente permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche.
- (10) La direttiva 2011/24/UE del Parlamento europeo e del Consiglio <sup>(3)</sup> istituisce una rete di autorità nazionali responsabili dell'assistenza sanitaria online. Per migliorare la sicurezza e la continuità dell'assistenza sanitaria transfrontaliera, tale rete deve elaborare orientamenti sull'accesso transfrontaliero ai dati e ai servizi elettronici, anche sostenendo «misure comuni di identificazione e autenticazione per agevolare la trasferibilità dei dati nell'assistenza sanitaria transfrontaliera». Il riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica è un fattore essenziale per realizzare l'assistenza sanitaria transfrontaliera per i cittadini europei. Quando i cittadini viaggiano per ottenere assistenza medica, la loro cartella clinica deve essere accessibile nel paese in cui si sottopongono alle cure. Ciò richiede un quadro di identificazione elettronica solido, sicuro e affidabile.
- (11) Il presente regolamento dovrebbe essere applicato nel pieno rispetto dei principi relativi alla protezione dei dati personali ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio <sup>(4)</sup>. A tale riguardo, per quanto concerne il principio del riconoscimento reciproco stabilito dal presente regolamento, l'autenticazione in un servizio online dovrebbe riguardare esclusivamente il trattamento di dati di identificazione che siano adeguati, pertinenti e non eccedenti per garantire l'accesso a detto servizio online. Inoltre, gli obblighi previsti dalla direttiva 95/46/CE in materia di riservatezza e sicurezza dei trattamenti dovrebbero essere rispettati dai prestatori di servizi fiduciari e dagli organismi di vigilanza.
- (12) Un obiettivo del presente regolamento è l'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici. Il presente regolamento non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri. Lo scopo del presente regolamento è garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

<sup>(1)</sup> GU C 50 E del 21.2.2012, pag. 1.

<sup>(2)</sup> Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno (GU L 376 del 27.12.2006, pag. 36).

<sup>(3)</sup> Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

<sup>(4)</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

- (13) È opportuno che gli Stati membri rimangano liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, e che possano decidere dell'eventuale partecipazione del settore privato nell'offerta di tali mezzi. È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione. Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici.
- (14) Occorre che il presente regolamento fissi talune condizioni in merito all'obbligo di riconoscimento dei mezzi di identificazione elettronica e alle modalità di notifica dei regimi di identificazione elettronica. È opportuno che tali condizioni aiutino gli Stati membri a costruire la necessaria fiducia nei rispettivi regimi di identificazione elettronica e a riconoscere reciprocamente i mezzi di identificazione elettronica che fanno parte dei regimi notificati. È opportuno che il principio del riconoscimento reciproco si applichi ove il regime di identificazione elettronica dello Stato membro notificante soddisfi le condizioni di notifica e la notifica sia stata pubblicata nella *Gazzetta ufficiale dell'Unione europea*. Tuttavia, il principio del riconoscimento reciproco dovrebbe riguardare esclusivamente l'autenticazione nei servizi online. È opportuno che l'accesso a tali servizi online e la loro fornitura finale al richiedente siano strettamente collegati al diritto a usufruire di tali servizi alle condizioni fissate nel diritto nazionale.
- (15) L'obbligo di riconoscere i mezzi di identificazione elettronica dovrebbe riferirsi esclusivamente ai mezzi il cui livello di garanzia dell'identità corrisponde a un livello pari o superiore a quello richiesto per il servizio online in questione. Inoltre, tale obbligo dovrebbe applicarsi solo qualora l'organismo del settore pubblico in questione utilizzi il livello di garanzia «significativo» o «elevato» in relazione all'accesso a tale servizio online. È opportuno che gli Stati membri mantengano la libertà, conformemente al diritto comunitario, di riconoscere mezzi di identificazione elettronica aventi livelli di garanzia dell'identità inferiori.
- (16) I livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata. Il livello di garanzia dipende dal grado di sicurezza fornito dai mezzi di identificazione elettronica riguardo all'identità pretesa o dichiarata di una persona tenendo conto dei procedimenti (ad esempio, controllo e verifica dell'identità, e autenticazione), delle attività di gestione (ad esempio, l'entità che rilascia i mezzi di identificazione elettronica e la procedura di rilascio di tali mezzi) e dei controlli tecnici messi in atto. Come risultato dei progetti pilota su larga scala finanziati dall'Unione, della normazione e di attività a livello internazionale, esistono varie definizioni e descrizioni tecniche dei livelli di garanzia. In particolare, il progetto pilota su larga scala STORK e la norma ISO 29115 fanno riferimento, tra l'altro, ai livelli 2, 3 e 4, che dovrebbero essere tenuti nella massima considerazione all'atto di stabilire le norme, le procedure e i requisiti tecnici minimi per i livelli di garanzia basso, significativo ed elevato ai sensi del presente regolamento, assicurando al contempo l'applicazione coerente del presente regolamento in particolare per quanto riguarda il livello di garanzia elevato in relazione al controllo dell'identità ai fini del rilascio di certificati qualificati. I requisiti stabiliti dovrebbero essere neutrali dal punto di vista tecnologico. Dovrebbe essere possibile soddisfare i requisiti di sicurezza necessari attraverso tecnologie differenti.
- (17) È opportuno che gli Stati membri incoraggino il settore privato a impiegare volontariamente mezzi di identificazione elettronica nell'ambito di un regime notificato a fini di identificazione ove necessario per servizi online o transazioni elettroniche. La facoltà di ricorrere a tali mezzi di identificazione elettronica consentirebbe al settore privato di avvalersi dell'identificazione e autenticazione elettroniche già ampiamente impiegate in molti Stati membri almeno per i servizi pubblici e di agevolare alle imprese e ai cittadini l'accesso transfrontaliero ai loro servizi online. Per facilitare l'impiego transfrontaliero di tali mezzi di identificazione elettronica da parte del settore privato, è opportuno che la possibilità di autenticazione offerta da uno Stato membro sia disponibile alle parti del settore privato facenti affidamento sulla certificazione stabilite al di fuori del territorio di detto Stato membro alle stesse condizioni applicate alle parti del settore privato facenti affidamento sulla certificazione stabilite nel suddetto Stato membro. Di conseguenza, per quanto riguarda le parti del settore privato facenti affidamento sulla certificazione, lo Stato membro notificante può definire termini di accesso ai mezzi di autenticazione. Detti termini di accesso possono indicare se i mezzi di autenticazione relativi al regime notificato sono attualmente disponibili alle parti del settore privato facenti affidamento sulla certificazione.
- (18) Il presente regolamento dovrebbe prevedere la responsabilità dello Stato membro notificante, della parte che rilascia i mezzi di identificazione elettronica e della parte che gestisce la procedura di autenticazione per mancato rispetto degli obblighi pertinenti a norma del presente regolamento. Tuttavia, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali in materia di responsabilità. Pertanto esso non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni o alle pertinenti norme procedurali applicabili, incluso l'onere della prova.

- (19) La sicurezza dei regimi di identificazione elettronica è fondamentale per un affidabile riconoscimento reciproco transfrontaliero dei mezzi di identificazione elettronica. In tale contesto, gli Stati membri dovrebbero cooperare in materia di sicurezza e interoperabilità dei regimi di identificazione elettronica a livello dell'Unione. Ogniqualvolta i regimi di identificazione elettronica richiedano alle parti che fanno affidamento sulla certificazione di utilizzare hardware o software specifici a livello nazionale, l'interoperabilità transfrontaliera richiede che tali Stati membri non impongano tali requisiti e le spese relative alle parti facenti affidamento sulla certificazione stabilite al di fuori del loro territorio. In tal caso si dovrebbero esaminare ed elaborare soluzioni appropriate nell'ambito del quadro di interoperabilità. Tuttavia, sono inevitabili i requisiti tecnici derivanti dalle specifiche inerenti ai mezzi di identificazione elettronica nazionali e suscettibili di avere ripercussioni per i detentori di tali mezzi elettronici (ad esempio, le smart card).
- (20) È opportuno che la cooperazione degli Stati membri agevoli l'interoperabilità tecnica dei regimi di identificazione elettronica notificati, al fine di promuovere un elevato livello di fiducia e sicurezza, in funzione del grado di rischio. È opportuno che lo scambio di informazioni e la condivisione delle migliori prassi fra Stati membri, finalizzati al riconoscimento reciproco dei regimi, facilitino tale cooperazione.
- (21) È anche opportuno che il presente regolamento istituisca un quadro giuridico generale per l'impiego dei servizi fiduciari. Tuttavia, non è opportuno che istituisca un obbligo generale di farne uso o che installi un punto di accesso per tutti i servizi fiduciari esistenti. In particolare, non è auspicabile che il regolamento copra la prestazione di servizi fiduciari usati esclusivamente nell'ambito di sistemi chiusi da un insieme definito di partecipanti che non hanno ripercussioni su terzi. Ad esempio, i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal presente regolamento. Solo i servizi fiduciari prestati al pubblico aventi ripercussioni su terzi dovrebbero soddisfare i requisiti previsti dal presente regolamento. Non è neanche auspicabile che il presente regolamento copra aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici nei casi in cui la normativa nazionale o unionale stabilisca obblighi quanto alla forma. Inoltre, non dovrebbe avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali.
- (22) Al fine di contribuire al loro impiego transfrontaliero generale, è opportuno che sia possibile utilizzare i servizi fiduciari come prove in procedimenti giudiziali in tutti gli Stati membri. Spetta al diritto nazionale definire gli effetti giuridici dei servizi fiduciari, salvo che il presente regolamento provveda altrimenti.
- (23) Nella misura in cui il presente regolamento disponga l'obbligo di riconoscere un servizio fiduciario, tale servizio fiduciario può essere rifiutato solo qualora il destinatario dell'obbligo non sia in grado di leggerlo o verificarlo per motivi tecnici che sfuggono al suo immediato controllo. Tuttavia, tale obbligo non dovrebbe di per se stesso esigere che un organismo pubblico ottenga l'hardware e il software necessari per la leggibilità tecnica di tutti i servizi fiduciari esistenti.
- (24) Gli Stati membri possono mantenere o introdurre disposizioni nazionali, conformemente al diritto dell'Unione, in materia di servizi fiduciari, nella misura in cui detti servizi non siano pienamente armonizzati dal presente regolamento. Tuttavia, i servizi fiduciari conformi al presente regolamento dovrebbero godere della libera circolazione nel mercato interno.
- (25) È opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quali servizi fiduciari qualificati.
- (26) In considerazione del ritmo dei mutamenti tecnologici, occorre che il presente regolamento adotti un approccio aperto all'innovazione.
- (27) È opportuno che il presente regolamento sia neutrale sotto il profilo tecnologico. È auspicabile che gli effetti giuridici prodotti dal presente regolamento siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti.

- (28) Al fine di migliorare in particolare la fiducia delle piccole e medie imprese (PMI) e dei consumatori nel mercato interno e di promuovere l'impiego dei servizi e prodotti fiduciari, è opportuno introdurre le nozioni di servizi fiduciari qualificati e di prestatori di servizi fiduciari qualificati, per precisare i requisiti e gli obblighi che garantiscano un elevato livello di sicurezza di tutti i servizi e prodotti fiduciari qualificati impiegati o prestati.
- (29) In linea con gli obblighi assunti a norma della Convenzione delle Nazioni Unite per i diritti delle persone con disabilità, approvata con decisione 2010/48/CE del Consiglio <sup>(1)</sup>, in particolare l'articolo 9 della Convenzione, le persone con disabilità dovrebbero poter utilizzare servizi fiduciari e prodotti destinati al consumatore finale impiegati nella prestazione di tali servizi alle stesse condizioni degli altri consumatori. Ove fattibile, pertanto, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi dovrebbero essere resi accessibili alle persone con disabilità. La valutazione di fattibilità dovrebbe includere considerazioni tecniche ed economiche.
- (30) Gli Stati membri dovrebbero designare uno o più organismi di vigilanza per lo svolgimento delle attività di vigilanza previste dal presente regolamento. Gli Stati membri dovrebbero altresì avere facoltà di decidere, di comune accordo con un altro Stato membro, di designare un organismo di vigilanza nel territorio di tale altro Stato membro.
- (31) Gli organismi di vigilanza dovrebbero cooperare con le autorità di protezione dei dati, ad esempio informandole in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali. In particolare, è opportuno che la trasmissione di informazioni copra gli incidenti di sicurezza e le violazioni dei dati personali.
- (32) È opportuno che tutti i prestatori di servizi fiduciari adottino buone prassi di sicurezza in funzione dei rischi connessi con le loro attività, in modo da migliorare la fiducia degli utilizzatori nel mercato unico.
- (33) È opportuno che le disposizioni sull'uso degli pseudonimi nei certificati non impediscano agli Stati membri di chiedere l'identificazione delle persone in base alla normativa unionale o nazionale.
- (34) È opportuno che tutti gli Stati membri si adeguino a requisiti essenziali comuni di vigilanza per garantire un livello paragonabile di sicurezza dei servizi fiduciari qualificati. Per facilitare l'applicazione coerente di tali requisiti in tutta l'Unione occorre che gli Stati membri adottino procedure paragonabili e scambino informazioni sulle loro attività di vigilanza e sulle migliori prassi del settore.
- (35) Tutti i prestatori di servizi fiduciari dovrebbero essere soggetti ai requisiti del presente regolamento, in particolare a quelli in materia di sicurezza e responsabilità, al fine di garantire la dovuta diligenza, la trasparenza e l'attendibilità delle loro operazioni e servizi. Tuttavia, tenendo conto del tipo di servizi fornito dai prestatori di servizi fiduciari, per quanto riguarda tali requisiti è opportuno distinguere tra servizi fiduciari qualificati e non qualificati.
- (36) L'istituzione di un regime di vigilanza per tutti i prestatori di servizi fiduciari dovrebbe assicurare parità di condizioni per la sicurezza e l'attendibilità delle loro operazioni e servizi, contribuendo in tal modo alla tutela degli utenti e al funzionamento del mercato interno. I prestatori di servizi fiduciari non qualificati dovrebbero essere soggetti ad attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. Pertanto l'organismo di sorveglianza non dovrebbe avere un obbligo generale di vigilanza sui prestatori di servizi non qualificati. L'organismo di sorveglianza dovrebbe adottare misure solo quando viene informato (ad esempio, dallo stesso prestatore di servizi fiduciari non qualificati, da un altro organismo di sorveglianza, mediante la notifica di un utente o di un partner commerciale o in base a sue indagini proprie) che un prestatore di servizi fiduciari non qualificato non soddisfa i requisiti del presente regolamento.

<sup>(1)</sup> Decisione 2010/48/CE del Consiglio, del 26 novembre 2009, relativa alla conclusione, da parte della Comunità europea, della convenzione delle Nazioni Unite sui diritti delle persone con disabilità (GU L 23 del 27.1.2010, pag. 35).

- (37) Il presente regolamento dovrebbe prevedere la responsabilità di tutti i prestatori di servizi fiduciari. In particolare, stabilisce il regime di responsabilità in base al quale tutti i prestatori di servizi fiduciari dovrebbero essere responsabili dei danni provocati a persone fisiche o giuridiche a causa del mancato rispetto degli obblighi previsti dal presente regolamento. Al fine di agevolare la valutazione del rischio finanziario che i prestatori di servizi fiduciari possano dover sostenere o che debbano coprire con polizze assicurative, il presente regolamento autorizza i prestatori di servizi fiduciari a stabilire limiti, a talune condizioni, all'uso dei servizi da essi prestati e non essere pertanto responsabili dei danni derivanti dall'uso dei servizi oltre i suddetti limiti. I clienti dovrebbero essere debitamente e anticipatamente informati di tali limiti. Tali limiti dovrebbero essere riconoscibili per i terzi, ad esempio inserendo informazioni sui limiti nei termini e nelle condizioni del servizio prestato o attraverso altri mezzi riconoscibili. Allo scopo di dare effetto a tali principi, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali sulla responsabilità. Pertanto, il presente regolamento non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni, del dolo, della negligenza o alle pertinenti norme procedurali applicabili.
- (38) La notifica delle violazioni di sicurezza e delle valutazioni di rischio per la sicurezza è essenziale per fornire informazioni adeguate alle parti interessate in caso di violazione di sicurezza o perdita di integrità.
- (39) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di notifica delle violazioni di cui al presente regolamento, è opportuno imporre l'obbligo agli organismi di vigilanza di fornire informazioni riassuntive alla Commissione e all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).
- (40) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di vigilanza perfezionato di cui al presente regolamento, è opportuno chiedere agli organismi di vigilanza di riferire sulle loro attività. Ciò servirebbe ad agevolare lo scambio di buone prassi fra organismi di vigilanza e consentirebbe di verificare l'applicazione coerente ed efficiente dei requisiti essenziali di vigilanza in tutti gli Stati membri.
- (41) Per garantire che i servizi fiduciari qualificati siano sostenibili e duraturi e migliorare la fiducia degli utilizzatori nella continuità di detti servizi, è opportuno che gli organismi di vigilanza verifichino l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nel caso in cui prestatori di servizi fiduciari qualificati cessino le loro attività.
- (42) Per facilitare la vigilanza sui prestatori di servizi fiduciari qualificati, ad esempio allorché un prestatore offre i suoi servizi sul territorio di uno Stato membro in cui non è soggetto a vigilanza o qualora i computer di un prestatore siano situati nel territorio di uno Stato membro diverso da quello in cui il prestatore è stabilito, è opportuno istituire un sistema di assistenza mutua fra gli organismi di vigilanza negli Stati membri.
- (43) Al fine di assicurare la conformità dei prestatori di servizi fiduciari qualificati e dei servizi da essi prestati ai requisiti stabiliti dal presente regolamento, un organismo di valutazione della conformità dovrebbe effettuare una valutazione della conformità; i prestatori di servizi fiduciari qualificati dovrebbero trasmettere all'organismo di vigilanza le relazioni di valutazione di conformità risultanti. Ogniqualevolta l'organismo di vigilanza richieda a un prestatore di servizi fiduciari qualificato di presentare una relazione di valutazione di conformità ad hoc, l'organismo di vigilanza dovrebbe rispettare in particolare i principi di buona amministrazione, compreso l'obbligo di fornire le motivazioni delle sue decisioni, nonché il principio di proporzionalità. Pertanto, l'organismo di vigilanza dovrebbe debitamente giustificare la propria decisione di imporre una valutazione di conformità ad hoc.
- (44) Il presente regolamento mira a garantire un quadro coerente affinché i servizi fiduciari siano dotati di un livello elevato di sicurezza e certezza giuridica. A tale riguardo, nel trattare la valutazione di conformità di prodotti e servizi, la Commissione dovrebbe, ove opportuno, cercare sinergie con i pertinenti regimi europei e internazionali vigenti, quali il regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio <sup>(1)</sup> che sancisce gli obblighi in materia di accreditamento degli organismi di valutazione della conformità e vigilanza del mercato di prodotti.

<sup>(1)</sup> Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).



- (45) Per consentire un processo di avviamento efficiente, che conduca all'inclusione dei prestatori di servizi fiduciari qualificati e dei servizi fiduciari qualificati da essi offerti negli elenchi di fiducia, è opportuno incoraggiare interazioni preliminari fra gli aspiranti prestatori di servizi fiduciari qualificati e l'organismo di vigilanza competente, in vista di facilitare l'esercizio della dovuta diligenza nell'offerta di servizi fiduciari qualificati.
- (46) Gli elenchi di fiducia sono elementi essenziali nel costruire la fiducia fra operatori di mercato perché indicano la condizione qualificata del prestatore di servizi al momento della vigilanza.
- (47) La fiducia nei servizi online e la loro agevolezza sono essenziali perché gli utilizzatori possano beneficiare a pieno dei servizi elettronici e avvalersi consapevolmente di essi. A tale scopo si dovrebbe creare un marchio di fiducia UE per individuare i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati. Tale marchio di fiducia UE per i servizi fiduciari qualificati distinguerebbe chiaramente i servizi fiduciari qualificati da altri servizi fiduciari, contribuendo così alla trasparenza sul mercato. L'utilizzo di un marchio di fiducia UE da parte dei prestatori di servizi fiduciari qualificati dovrebbe essere volontario e non dovrebbe implicare requisiti aggiuntivi diversi da quelli previsti dal presente regolamento.
- (48) Sebbene sia necessario un elevato livello di sicurezza per garantire il riconoscimento reciproco delle firme elettroniche, in casi specifici come nel contesto della decisione 2009/767/CE della Commissione <sup>(1)</sup>, è opportuno che siano accettate anche firme elettroniche con una garanzia di sicurezza più debole.
- (49) Il presente regolamento dovrebbe stabilire il principio secondo il quale alla firma elettronica non dovrebbero essere negati gli effetti giuridici per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal presente regolamento secondo cui una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa.
- (50) Poiché attualmente le autorità competenti negli Stati membri utilizzano formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti, occorre garantire che almeno alcuni formati di firma elettronica possano essere supportati tecnicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente. Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di sigillo elettronico avanzato.
- (51) È opportuno che il firmatario possa affidare a terzi i dispositivi per la creazione di una firma elettronica qualificata, purché siano rispettati appropriati meccanismi e procedure per garantire che il firmatario mantenga il controllo esclusivo sull'uso dei suoi dati di creazione di firma elettronica e l'uso del dispositivo soddisfi i requisiti della firma elettronica qualificata.
- (52) Visti i suoi molteplici vantaggi economici, sarà ulteriormente sviluppata la creazione di firme elettroniche a distanza, qualora l'ambiente di creazione di firma elettronica sia gestito da un prestatore di servizi fiduciari a nome del firmatario. Tuttavia, per garantire che alle firme elettroniche sia attribuito lo stesso riconoscimento giuridico delle firme elettroniche create con un ambiente interamente gestito dall'utente, i prestatori che offrono servizi di firma elettronica a distanza dovrebbero applicare procedure di sicurezza di gestione e amministrative specifiche e utilizzare sistemi e prodotti affidabili, che in particolare comprendano canali di comunicazione elettronici sicuri per garantire l'affidabilità dell'ambiente di creazione di firma elettronica e assicurare che sia utilizzato sotto il controllo esclusivo del firmatario. Nel caso di una firma elettronica qualificata creata mediante un dispositivo di creazione di firma elettronica a distanza, dovrebbero applicarsi i requisiti applicabili ai prestatori di servizi fiduciari qualificati, stabiliti dal presente regolamento.

<sup>(1)</sup> Decisione 2009/767/CE della Commissione, del 16 ottobre 2009, che stabilisce misure per facilitare l'uso di procedure per via elettronica mediante gli «sportelli unici» di cui alla direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno (GU L 274 del 20.10.2009, pag. 36).

- (53) La sospensione dei certificati qualificati è una prassi operativa abituale dei prestatori di servizi fiduciari in una serie di Stati membri, che è diversa dalla revoca e comporta la perdita di validità temporanea di un certificato. La certezza del diritto richiede che la situazione di sospensione di un certificato sia sempre indicata chiaramente. A tale scopo i prestatori di servizi fiduciari dovrebbero avere la responsabilità di indicare chiaramente la situazione del certificato e, in caso di sospensione, il periodo di tempo esatto durante il quale il certificato è sospeso. È opportuno che il presente regolamento non imponga ai prestatori di servizi fiduciari o agli Stati membri l'utilizzo della sospensione, ma preveda norme di trasparenza nei casi in cui tale prassi è disponibile.
- (54) L'interoperabilità transfrontaliera e il riconoscimento dei certificati qualificati è una condizione essenziale per il riconoscimento transfrontaliero delle firme elettroniche qualificate. Pertanto, i certificati qualificati non dovrebbero essere soggetti a requisiti obbligatori oltre ai requisiti di cui al presente regolamento. Tuttavia, a livello nazionale, dovrebbe essere consentita l'inclusione di attributi specifici, quali identificatori unici, nei certificati qualificati, purché tali attributi specifici non ostacolino l'interoperabilità transfrontaliera e il riconoscimento dei certificati e delle firme elettroniche qualificate.
- (55) La certificazione della sicurezza delle tecnologie d'informazione basata su norme internazionali, come l'ISO 15408 e i metodi di valutazione e le disposizioni di riconoscimento reciproco connessi, è uno strumento importante per verificare la sicurezza dei dispositivi per la creazione di una firma elettronica qualificata e dovrebbe essere promossa. Soluzioni e servizi innovativi, quali la firma in cloud e la firma mobile, tuttavia, si basano su soluzioni tecniche e organizzative per dispositivi per la creazione di una firma elettronica qualificata per i quali possono non essere ancora disponibili norme di sicurezza o per i quali può essere in corso la prima certificazione della sicurezza delle tecnologie d'informazione. Il livello di sicurezza di tali dispositivi per la creazione di una firma elettronica qualificata potrebbe essere valutato utilizzando procedure alternative solo se tali norme di sicurezza non sono disponibili o se la prima certificazione della sicurezza delle tecnologie d'informazione è in corso. Tali processi dovrebbero essere comparabili alle norme per la certificazione della sicurezza delle tecnologie d'informazione sempre che i livelli di sicurezza siano equivalenti. Tali processi potrebbero essere agevolati da una revisione tra pari.
- (56) Il presente regolamento dovrebbe stabilire i requisiti relativi a dispositivi per la creazione di una firma elettronica qualificata al fine di assicurare la funzionalità delle firme elettroniche avanzate. Il presente regolamento non dovrebbe contemplare la globalità dell'ambiente del sistema in cui tali dispositivi operano. Pertanto, l'ambito di applicazione della certificazione dei dispositivi per la creazione di una firma qualificata dovrebbe essere limitato all'hardware e al software di sistema utilizzato per gestire e proteggere i dati per la creazione di una firma elettronica creati, memorizzati o trattati nel dispositivo di creazione di una firma. Come specificato nelle norme pertinenti, l'ambito di applicazione dell'obbligo di certificazione dovrebbe escludere le applicazioni relative alla creazione di una firma.
- (57) Per garantire la certezza giuridica della validità della firma, è essenziale specificare i componenti di una firma elettronica qualificata, che dovrebbero essere valutati dalla parte facente affidamento sulla certificazione che effettua la convalida. Inoltre, è opportuno che attraverso la specificazione degli obblighi dei prestatori di servizi fiduciari qualificati che possono offrire un servizio di convalida qualificata a parti facenti affidamento sulla certificazione che non vogliono o non possono effettuare esse stesse la convalida di firme elettroniche qualificate siano stimolati gli investimenti del settore privato e pubblico in tali servizi. È opportuno che entrambi gli elementi rendano la convalida delle firme elettroniche qualificate semplice e agevole per tutte le parti a livello dell'Unione.
- (58) Qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.
- (59) È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.
- (60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di sigilli elettronici dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di sigillo elettronico, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.



- (61) È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.
- (62) Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti nel presente regolamento.
- (63) I documenti elettronici sono importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.
- (64) Nel trattare i formati delle firme e dei sigilli elettronici avanzati, la Commissione dovrebbe basarsi sulle prassi, sulle norme e sulla legislazione esistente, in particolare la decisione 2011/130/UE della Commissione <sup>(1)</sup>.
- (65) Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server.
- (66) È essenziale prevedere un quadro giuridico per agevolare il riconoscimento transfrontaliero tra gli ordinamenti giuridici nazionali esistenti relativi ai servizi elettronici di recapito certificato. Tale quadro potrebbe aprire inoltre per i prestatori di servizi fiduciari dell'Unione nuove opportunità di mercato per l'offerta di nuovi servizi elettronici di recapito certificati paneuropei.
- (67) I servizi di autenticazione dei siti web prevedono un mezzo tramite il quale il visitatore di un sito può accertarsi che dietro a quel sito web vi è un'entità reale e legittima. Tali servizi contribuiscono a diffondere sicurezza e fiducia nelle transazioni commerciali on line, in quanto gli utenti si fideranno di un sito web che è stato autenticato. La fornitura e l'uso di servizi di autenticazione dei siti web sono interamente volontari. Tuttavia, affinché l'autenticazione dei siti web divenga un mezzo per rafforzare la fiducia, fornire un'esperienza migliore all'utente e promuovere la crescita nel mercato interno, è opportuno che il presente regolamento stabilisca obblighi minimi in materia di sicurezza e responsabilità per i prestatori e i loro servizi. A tal fine, si è tenuto conto dei risultati delle iniziative industriali esistenti, ad esempio, il Forum Autorità di certificazione/Browser (CA/B Forum). Inoltre, il presente regolamento non dovrebbe impedire l'uso di altri mezzi o metodi di autenticazione di un sito web non rientranti nel presente regolamento e non dovrebbe vietare ai prestatori di servizi di autenticazione dei siti web di paesi terzi di prestare i propri servizi ai clienti dell'Unione. Tuttavia, i servizi di autenticazione dei siti web di un prestatore di un paese terzo dovrebbero essere riconosciuti come qualificati ai sensi del presente regolamento solo se è stato concluso un accordo internazionale tra l'Unione e il paese di stabilimento di detto prestatore.
- (68) La nozione di «persone giuridiche» secondo le disposizioni del trattato sul funzionamento dell'Unione europea (TFUE) in materia di stabilimento lascia agli operatori la libertà di scegliere la forma giuridica che ritengono opportuna per svolgere la loro attività. Di conseguenza, per «persone giuridiche» ai sensi del TFUE si intendono tutte le entità costituite conformemente al diritto di uno Stato membro o da esso disciplinate, a prescindere dalla loro forma giuridica.
- (69) Le istituzioni, gli organi, gli uffici e le agenzie dell'Unione sono incoraggiate a riconoscere l'identificazione elettronica e i servizi fiduciari contemplati dal presente regolamento ai fini dell'amministrazione cooperativa facendo tesoro, in particolare, delle buone prassi esistenti e dei risultati dei progetti in corso nei settori contemplati dal presente regolamento.

<sup>(1)</sup> Decisione 2011/130/UE della Commissione, del 25 febbraio 2011, che istituisce requisiti minimi per il trattamento transfrontaliero dei documenti firmati elettronicamente dalle autorità competenti a norma della direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno (GU L 53 del 26.2.2011, pag. 66).

- (70) Al fine di completare determinati aspetti tecnici dettagliati del presente regolamento in modo flessibile e veloce, dovrebbe essere delegato alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE riguardo ai criteri che devono soddisfare gli organismi responsabili della certificazione dei dispositivi per la creazione di una firma elettronica qualificata. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.
- (71) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione, in particolare per specificare i numeri di riferimento delle norme il cui impiego conferisce una presunzione di adempimento di determinati requisiti stabiliti nel presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio <sup>(1)</sup>.
- (72) In sede di elaborazione degli atti delegati o di esecuzione, la Commissione dovrebbe tenere debito conto delle norme e delle specifiche tecniche elaborate da organizzazioni e organismi di normalizzazione europei e internazionali, in particolare il Comitato europeo di normalizzazione (CEN), l'Istituto europeo delle norme di telecomunicazione (ETSI), l'Organizzazione internazionale per la standardizzazione (ISO) e l'Unione internazionale delle telecomunicazioni (UIT), al fine di assicurare un livello elevato di sicurezza e interoperabilità dell'identificazione elettronica e dei servizi fiduciari.
- (73) Per motivi di certezza del diritto e di chiarezza è opportuno abrogare la direttiva 1999/93/CE.
- (74) Per garantire la certezza giuridica per operatori di mercato che già fanno uso di certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE, è necessario prevedere un idoneo periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per i dispositivi per la creazione di una firma sicura, la cui conformità sia stata determinata ai sensi della direttiva 1999/93/CE, nonché per i prestatori di servizi di certificazione che rilasciano certificati qualificati entro il 1° luglio 2016. Infine, è altresì necessario dotare la Commissione dei mezzi per adottare atti di esecuzione e atti delegati prima di tale data.
- (75) Le date di applicazione stabilite nel presente regolamento non pregiudicano gli obblighi esistenti già contratti dagli Stati membri in base al diritto dell'Unione, in particolare della direttiva 2006/123/CE.
- (76) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della portata dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
- (77) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio <sup>(2)</sup> e ha espresso un parere il 27 settembre 2012 <sup>(3)</sup>,

<sup>(1)</sup> Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

<sup>(2)</sup> Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

<sup>(3)</sup> GU C 28 del 30.1.2013, pag. 6.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

**DISPOSIZIONI GENERALI**

*Articolo 1*

**Oggetto**

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:

- a) fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,
- b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e
- c) istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

*Articolo 2*

**Ambito di applicazione**

- 1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.
- 2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.
- 3. Il presente regolamento non pregiudica il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.

*Articolo 3*

**Definizioni**

Ai fini del presente regolamento si intende per:

- 1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;
- 2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;
- 3) «dati di identificazione personale», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;
- 4) «regime di identificazione elettronica», un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;

- 5) «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;
- 6) «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;
- 7) «organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;
- 8) «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio <sup>(1)</sup>;
- 9) «firmatario», una persona fisica che crea una firma elettronica;
- 10) «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;
- 11) «firma elettronica avanzata», una firma elettronica che soddisfa i requisiti di cui all'articolo 26;
- 12) «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;
- 13) «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;
- 14) «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;
- 15) «certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;
- 16) «servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:
  - a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
  - b) creazione, verifica e convalida di certificati di autenticazione di siti web; o
  - c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;
- 17) «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

<sup>(1)</sup> Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

- 18) «organismo di valutazione della conformità», un organismo ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;
- 19) «prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;
- 20) «prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;
- 21) «prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;
- 22) «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;
- 23) «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;
- 24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;
- 25) «sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;
- 26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfa i requisiti sanciti all'articolo 36;
- 27) «sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;
- 28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;
- 29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;
- 30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;
- 31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;
- 32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;
- 33) «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
- 34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

- 35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
- 36) «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;
- 37) «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;
- 38) «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;
- 39) «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;
- 40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;
- 41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

#### Articolo 4

##### **Principio del mercato interno**

1. Non sono imposte restrizioni alla prestazione di servizi fiduciari nel territorio di uno Stato membro da parte di un prestatore di servizi fiduciari stabilito in un altro Stato membro per motivi che rientrano negli ambiti di applicazione del presente regolamento.
2. I prodotti e i servizi fiduciari conformi al presente regolamento godono della libera circolazione nel mercato interno.

#### Articolo 5

##### **Trattamento e protezione dei dati**

1. Il trattamento dei dati a carattere personale è effettuato a norma della direttiva 95/46/CE.
2. Fatti salvi gli effetti giuridici che il diritto nazionale attribuisce agli pseudonimi, gli Stati membri non vietano l'uso di pseudonimi nelle transazioni elettroniche.

#### CAPO II

##### **IDENTIFICAZIONE ELETTRONICA**

#### Articolo 6

##### **Riconoscimento reciproco**

1. Ove il diritto o la prassi amministrativa nazionale richiedano l'impiego di un'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro, i mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti nel primo Stato membro ai fini dell'autenticazione transfrontaliera di tale servizio online, purché soddisfino le seguenti condizioni:
  - a) i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9;



- b) il livello di garanzia dei mezzi di identificazione elettronica corrisponde a un livello di garanzia pari o superiore al livello di garanzia richiesto dall'organismo del settore pubblico competente per accedere al servizio online in questione nel primo Stato membro, sempre che il livello di garanzia di tali mezzi di identificazione elettronica corrisponda al livello di garanzia significativo o elevato;
- c) l'organismo del settore pubblico competente usa il livello di garanzia significativo o elevato in relazione all'accesso a tale servizio online.

Tale riconoscimento ha luogo non oltre 12 mesi dalla data in cui la Commissione pubblica l'elenco i di cui alla lettera a), primo comma.

2. Un mezzo di identificazione elettronica rilasciato nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9 e che corrisponde al livello di garanzia basso può essere riconosciuto dagli organismi del settore pubblico ai fini dell'autenticazione transfrontaliera del servizio prestato online da tali organismi.

#### *Articolo 7*

##### **Ammissibilità alla notifica dei regimi di identificazione elettronica**

Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:

- a) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica sono rilasciati:
  - i) dallo Stato membro notificante;
  - ii) su incarico dello Stato membro notificante; o
  - iii) a titolo indipendente dallo Stato membro notificante e sono riconosciuti da tale Stato membro;
- b) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico e che richiede l'identificazione elettronica nello Stato membro notificante;
- c) il regime di identificazione elettronica e i mezzi di identificazione elettronica rilasciati conformemente alle sue disposizioni soddisfano i requisiti di almeno uno dei livelli di garanzia stabiliti nell'atto di esecuzione di cui all'articolo 8, paragrafo 3;
- d) lo Stato membro notificante garantisce che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure relative al pertinente livello di garanzia definito nell'atto di esecuzione di cui all'articolo 8, paragrafo 3, alla persona fisica o giuridica di cui all'articolo 3, punto 1, al momento in cui è rilasciata l'identificazione elettronica nell'ambito di detto regime;
- e) la parte che rilascia i mezzi di identificazione elettronica nell'ambito di detto regime assicura che i mezzi di identificazione elettronica siano attribuiti alla persona di cui alla lettera d) del presente articolo conformemente alle specifiche, norme e procedure tecniche relative al pertinente livello di garanzia definito nell'atto di esecuzione di cui all'articolo 8, paragrafo 3;
- f) lo Stato membro notificante garantisce la disponibilità dell'autenticazione online, per consentire alle parti facenti affidamento sulla certificazione stabilite nel territorio di un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica.

Per le parti facenti affidamento sulla certificazione diverse dagli organismi del settore pubblico, lo Stato membro notificante può definire i termini di accesso a tale autenticazione. Quando l'autenticazione transfrontaliera è effettuata in relazione a un servizio online prestato da un organismo del settore pubblico, essa è fornita a titolo gratuito.

Gli Stati membri non impongono alcun requisito tecnico specifico sproporzionato alle parti facenti affidamento sulla certificazione che intendono effettuare tale autenticazione, qualora tali requisiti impediscano o ostacolino notevolmente l'interoperabilità dei regimi di identificazione elettronica notificati;

- g) almeno sei mesi prima della notifica di cui all'articolo 9, paragrafo 1, lo Stato membro notificante fornisce agli altri Stati membri, ai fini dell'obbligo previsto dall'articolo 12, paragrafo 5, una descrizione di detto regime conformemente alle modalità procedurali stabilite dagli atti di esecuzione di cui all'articolo 12, paragrafo 7;
- h) il regime di identificazione elettronica soddisfa i requisiti definiti nell'atto di esecuzione di cui all'articolo 12, paragrafo 8.

#### Articolo 8

##### **Livelli di garanzia dei regimi di identificazione elettronica**

1. Un regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1, specifica livelli di garanzia basso, significativo e/o elevato per i mezzi di identificazione elettronica rilasciati nell'ambito di detto regime.
2. I livelli di garanzia basso, significativo e elevato soddisfano rispettivamente i seguenti criteri:
  - a) il livello di garanzia basso si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza limitato riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre il rischio di uso abusivo o alterazione dell'identità;
  - b) il livello di garanzia significativo si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza significativo riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre significativamente il rischio di uso abusivo o alterazione dell'identità;
  - c) il livello di garanzia elevato si riferisce a un mezzo di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza più elevato dei mezzi di identificazione elettronica aventi un livello di garanzia significativo ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità.
3. Entro il 18 settembre 2015, tenendo conto delle norme internazionali pertinenti e fatto salvo il paragrafo 2, la Commissione, mediante atti di esecuzione, definisce le specifiche, norme e procedure tecniche minime in riferimento alle quali sono specificati i livelli di garanzia basso, significativo e elevato dei mezzi di identificazione elettronica ai fini del paragrafo 1.

Le suddette specifiche, norme e procedure tecniche minime sono fissate facendo riferimento all'affidabilità e alla qualità dei seguenti elementi:

- a) della procedura di controllo e verifica dell'identità delle persone fisiche o giuridiche che chiedono il rilascio dei mezzi di identificazione elettronica;

- b) della procedura di rilascio dei mezzi di identificazione elettronica richiesti;
- c) del meccanismo di autenticazione mediante il quale la persona fisica o giuridica usa i mezzi di identificazione elettronica per confermare la propria identità a una parte facente affidamento sulla certificazione;
- d) dell'entità che rilascia i mezzi di identificazione elettronica;
- e) di qualsiasi altro organismo implicato nella domanda di rilascio dei mezzi di identificazione elettronica; e
- f) delle specifiche tecniche e di sicurezza dei mezzi di identificazione elettronica rilasciati.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### Articolo 9

##### **Notifica**

1. Lo Stato membro notificante rende note alla Commissione le informazioni seguenti e, senza indugio, qualsiasi loro successiva modifica:

- a) una descrizione del regime di identificazione elettronica, con indicazione dei suoi livelli di garanzia e della o delle entità che rilasciano i mezzi di identificazione elettronica nell'ambito del regime;
- b) il regime di vigilanza e il regime di informazioni sulla responsabilità applicabili per quanto riguarda:
  - i) la parte che rilascia i mezzi di identificazione elettronica; e
  - ii) la parte che gestisce la procedura di autenticazione;
- c) l'autorità o le autorità responsabili del regime di identificazione elettronica;
- d) informazioni sull'entità o sulle entità che gestiscono la registrazione dei dati unici di identificazione personale;
- e) una descrizione di come sono soddisfatti i requisiti definiti negli atti di esecuzione di cui all'articolo 12, paragrafo 8;
- f) una descrizione dell'autenticazione di cui all'articolo 7, lettera f);
- g) disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

2. Un anno dopo la data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco dei regimi di identificazione elettronica notificati ai sensi del paragrafo 1 del presente articolo e le informazioni fondamentali al riguardo.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco di cui al paragrafo 2 entro due mesi dalla data di ricezione di tale notifica.

4. Uno Stato membro può presentare alla Commissione una richiesta di eliminazione del regime di identificazione elettronica da esso notificato dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricezione della richiesta dello Stato membro.

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche a norma del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### Articolo 10

##### **Violazione della sicurezza**

1. In caso di violazione o parziale compromissione del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, o dell'autenticazione di cui all'articolo 7, lettera f), con limitazione dell'affidabilità dell'autenticazione transfrontaliera di tale regime, lo Stato membro notificante senza indugio sospende o revoca tale autenticazione transfrontaliera o le sue parti compromesse e ne informa gli altri Stati membri e la Commissione.

2. Una volta posto rimedio alla violazione o alla compromissione di cui al paragrafo 1, lo Stato membro notificante ristabilisce l'autenticazione transfrontaliera e informa senza indugio gli altri Stati membri e la Commissione.

3. Qualora non sia posto rimedio alla violazione o alla compromissione di cui al paragrafo 1 entro tre mesi dalla sospensione o dalla revoca, lo Stato membro notificante notifica agli altri Stati membri e alla Commissione il ritiro del regime di identificazione elettronica.

La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 9, paragrafo 2, nella *Gazzetta ufficiale dell'Unione europea*.

#### Articolo 11

##### **Responsabilità**

1. Lo Stato membro notificante è responsabile per i danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dei suoi obblighi di cui all'articolo 7, lettere d) e f), in una transazione transfrontaliera.

2. La parte che rilascia i mezzi di identificazione elettronica è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dell'obbligo di cui all'articolo 7, lettera e), in una transazione transfrontaliera.

3. La parte che gestisce la procedura di autenticazione è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica per non avere garantito la corretta gestione dell'autenticazione di cui all'articolo 7, lettera f), in una transazione transfrontaliera.

4. I paragrafi 1, 2 e 3 si applicano conformemente alle norme nazionali in materia di responsabilità.

5. I paragrafi 1, 2 e 3 lasciano impregiudicata la responsabilità conformemente al diritto nazionale delle parti di una transazione in cui sono utilizzati mezzi di identificazione elettronica che rientrano nel regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1.

#### Articolo 12

##### **Cooperazione e interoperabilità**

1. I regimi nazionali di identificazione elettronica notificati a norma dell'articolo 9, paragrafo 1, sono interoperabili.

2. È istituito un quadro di interoperabilità ai fini del paragrafo 1.

3. Il quadro di interoperabilità risponde ai seguenti criteri:

- a) mira a essere neutrale dal punto di vista tecnologico e non comporta discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro;
- b) segue, ove possibile, le norme europee e internazionali;
- c) facilita l'applicazione del principio della tutela della vita privata fin dalla progettazione (privacy by design); e
- d) garantisce che i dati personali siano trattati a norma della direttiva 95/46/CE.

4. Il quadro di interoperabilità è composto da:

- a) un riferimento ai requisiti tecnici minimi connessi ai livelli di garanzia di cui all'articolo 8;
- b) una mappatura dei livelli di garanzia nazionali dei regimi di identificazione elettronica notificati in base ai livelli di garanzia di cui all'articolo 8;
- c) un riferimento ai requisiti tecnici minimi di interoperabilità;
- d) un riferimento a un insieme minimo di dati di identificazione personale che rappresentano un'unica persona fisica o giuridica, disponibile nell'ambito dei regimi di identificazione elettronica;
- e) norme di procedura;
- f) disposizioni per la risoluzione delle controversie; e
- g) norme di sicurezza operativa comuni.

5. Gli Stati membri cooperano per quanto riguarda:

- a) l'interoperabilità dei regimi di identificazione elettronica notificati ai sensi dell'articolo 9, paragrafo 1, e dei regimi di identificazione elettronica che gli Stati membri intendono notificare; e
- b) la sicurezza dei regimi di identificazione elettronica.

6. La cooperazione fra gli Stati membri riguarda:

- a) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i regimi di identificazione elettronica e, in particolare, i requisiti tecnici connessi all'interoperabilità e ai livelli di garanzia;
- b) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i metodi di lavoro con i livelli di garanzia dei regimi di identificazione elettronica di cui all'articolo 8;
- c) la valutazione tra pari dei regimi di identificazione elettronica che rientrano nel presente regolamento; e
- d) l'esame degli sviluppi pertinenti nel settore dell'identificazione elettronica.

7. Entro il 18 marzo 2015, la Commissione, mediante atti di esecuzione, fissa le modalità procedurali necessarie per facilitare la collaborazione fra gli Stati membri di cui ai paragrafi 5 e 6, al fine di promuovere un elevato livello di fiducia e di sicurezza, commisurato al grado di rischio esistente.

8. Entro il 18 settembre 2015, al fine di garantire condizioni uniformi di esecuzione del requisito di cui al paragrafo 1, la Commissione, fatti salvi i criteri di cui al paragrafo 3 e tenendo conto dei risultati della cooperazione fra gli Stati membri, adotta atti di esecuzione sul quadro di interoperabilità quale definito al paragrafo 4.

9. Gli atti di esecuzione di cui ai paragrafi 7 e 8 sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

### CAPO III

## SERVIZI FIDUCIARI

### SEZIONE 1

#### *Disposizioni generali*

#### *Articolo 13*

#### **Responsabilità e onere della prova**

1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.

L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.

Si presume il dolo o la negligenza di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.

2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle limitazioni d'uso dei servizi da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati.

3. I paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità.

#### *Articolo 14*

#### **Relazioni internazionali**

1. I servizi fiduciari prestati da prestatori di servizi fiduciari stabiliti in un paese terzo sono riconosciuti giuridicamente equivalenti ai servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione qualora i servizi fiduciari aventi origine nel paese terzo siano riconosciuti a norma di un accordo concluso fra l'Unione e il paese terzo in questione o un'organizzazione internazionale a norma dell'articolo 218 TFUE.



2. Gli accordi di cui al paragrafo 1 garantiscono, in particolare, che:
  - a) i requisiti che si applicano ai prestatori di servizi fiduciari qualificati stabiliti nell'Unione e ai servizi fiduciari qualificati che prestano siano soddisfatti dai prestatori di servizi fiduciari nel paese terzo o presso le organizzazioni internazionali con cui è concluso l'accordo, nonché dai servizi fiduciari da essi prestati;
  - b) i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione sono riconosciuti come giuridicamente equivalenti ai servizi fiduciari prestati da prestatori di servizi fiduciari nel paese terzo o presso l'organizzazione internazionale con cui è concluso l'accordo.

#### *Articolo 15*

##### **Accessibilità per le persone con disabilità**

Ove possibile, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi sono resi accessibili alle persone con disabilità.

#### *Articolo 16*

##### **Sanzioni**

Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive.

#### *SEZIONE 2*

##### **Vigilanza**

#### *Articolo 17*

##### **Organismo di vigilanza**

1. Gli Stati membri designano un organismo di vigilanza stabilito nel loro territorio o, di comune accordo con un altro Stato membro, un organismo di vigilanza stabilito in tale altro Stato membro. Tale organismo è responsabile di compiti di vigilanza nello Stato membro designante.

Agli organismi di vigilanza sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dei rispettivi organismi di vigilanza designati.
3. Il ruolo dell'organismo di vigilanza è il seguente:
  - a) vigilare sui prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante per assicurarsi, mediante attività di vigilanza ex ante e ex post, che essi e i servizi fiduciari qualificati da essi prestati rispondano ai requisiti di cui al presente regolamento;
  - b) adottare misure, ove necessario, in relazione a prestatori di servizi fiduciari non qualificati stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora sia informato che tali prestatori di servizi fiduciari non qualificati o i servizi fiduciari da essi prestati presumibilmente non soddisfano i requisiti stabiliti dal presente regolamento.

4. Ai fini del paragrafo 3 e fatte salve le limitazioni ivi previste, l'organismo di vigilanza ha, in particolare, i compiti seguenti:

- a) cooperare con altri organismi di vigilanza e assisterli a norma dell'articolo 18;
- b) analizzare le relazioni di valutazione della conformità di cui all'articolo 20, paragrafo 1, e all'articolo 21, paragrafo 1;
- c) informare gli altri organismi di vigilanza e il pubblico in merito a violazioni della sicurezza o perdita di integrità a norma dell'articolo 19, paragrafo 2;
- d) riferire alla Commissione in merito alle sue principali attività a norma del paragrafo 6 del presente articolo;
- e) svolgere verifiche o chiedere a un organismo di valutazione della conformità di effettuare una valutazione di conformità dei prestatori di servizi fiduciari qualificati a norma dell'articolo 20, paragrafo 2;
- f) cooperare con le autorità di protezione, in particolare informandole senza indugio dei dati in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali;
- g) concedere la qualifica ai prestatori di servizi fiduciari e ai servizi da essi prestati e ritirare tale qualifica a norma degli articoli 20 e 21;
- h) informare l'organismo responsabile dell'elenco nazionale di fiducia di cui all'articolo 22, paragrafo 3, in merito alle proprie decisioni di concedere o ritirare la qualifica, salvo se tale organismo è anche l'organismo di vigilanza;
- i) verificare l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nei casi in cui il prestatore di servizi fiduciari qualificati cessa le sue attività, inclusi i modi in cui le informazioni sono mantenute accessibili a norma dell'articolo 24, paragrafo 2, lettera h);
- j) imporre ai prestatori di servizi fiduciari di rimediare a qualsiasi mancato adempimento dei requisiti di cui al presente regolamento.

5. Gli Stati membri possono imporre che l'organismo di vigilanza istituisca, mantenga e aggiorni un'infrastruttura fiduciaria secondo le condizioni di cui al diritto nazionale.

6. Entro il 31 marzo di ogni anno, ogni organismo di vigilanza presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile insieme a una sintesi delle notifiche di violazione ricevute da prestatori di servizi fiduciari a norma dell'articolo 19, paragrafo 2.

7. La Commissione mette a disposizione degli Stati membri la relazione annuale di cui al paragrafo 6.

8. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui al paragrafo 6. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*Articolo 18***Assistenza reciproca**

1. Gli organismi di vigilanza collaborano fra loro al fine di scambiarsi buone prassi.

Un organismo di vigilanza, previa ricezione di una richiesta giustificata da parte di un altro organismo di vigilanza, fornisce a quest'ultimo assistenza perché possano svolgere le attività di organismi di vigilanza in modo coerente. L'assistenza reciproca può coprire, in particolare, le richieste di informazioni e le misure di vigilanza, quali richieste di svolgere ispezioni in connessione con le relazioni di valutazione della conformità di cui agli articoli 20 e 21.

2. L'organismo di vigilanza cui è presentata una richiesta di assistenza può rifiutare tale richiesta per uno dei seguenti motivi:

- a) l'organismo di vigilanza non è competente a fornire l'assistenza richiesta;
- b) l'assistenza richiesta non è proporzionata alle attività di vigilanza dell'organismo di vigilanza svolte a norma dell'articolo 17;
- c) fornire l'assistenza richiesta sarebbe incompatibile con il presente regolamento.

3. Ove appropriato, gli Stati membri possono autorizzare i rispettivi organismi di vigilanza a svolgere indagini congiunte con la partecipazione di membri del personale di organismi di vigilanza di altri Stati membri. Le disposizioni e le procedure per tali indagini congiunte sono convenute e stabilite dagli Stati membri interessati conformemente al rispettivo diritto nazionale.

*Articolo 19***Requisiti di sicurezza relativi ai prestatori di servizi fiduciari**

1. I prestatori di servizi fiduciari qualificati e non qualificati adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali misure assicurano un livello di sicurezza commisurato al grado di rischio esistente. In particolare, sono adottate misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti.

2. Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, i prestatori di servizi fiduciari qualificati e non qualificati notificano all'organismo di vigilanza e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

Qualora sia probabile che la violazione della sicurezza o la perdita di integrità abbia effetti negativi su una persona fisica o giuridica a cui è stato prestato il servizio fiduciario, il prestatore di servizi fiduciari notifica senza indugio anche alla persona fisica o giuridica la violazione di sicurezza o la perdita di integrità.

Ove appropriato, in particolare qualora la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza notificato ne informa gli organismi di vigilanza negli altri Stati membri interessati e l'ENISA.

L'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico.

3. L'organismo di vigilanza trasmette all'ENISA, una volta all'anno, una sintesi delle notifiche di violazione di sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari.

4. La Commissione può, mediante atti di esecuzione:

- a) specificare ulteriormente le misure di cui al paragrafo 1; e
- b) definire i formati e le procedure, comprese le scadenze, applicabili ai fini del paragrafo 2.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

### SEZIONE 3

#### ***Servizi fiduciari qualificati***

##### *Articolo 20*

#### **Vigilanza dei prestatori di servizi fiduciari qualificati**

1. I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è di confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati soddisfano i requisiti di cui al presente regolamento. I prestatori di servizi fiduciari qualificati presentano la pertinente relazione di valutazione di conformità all'organismo di vigilanza entro il termine di tre giorni lavorativi dalla sua ricezione.

2. Fatto salvo il paragrafo 1, l'organismo di vigilanza può, in qualsiasi momento, condurre una verifica o chiedere a un organismo di valutazione della conformità di eseguire una valutazione di conformità dei prestatori di servizi fiduciari qualificati, a spese di tali prestatori di servizi fiduciari, per confermare che essi e i servizi fiduciari qualificati da essi prestati rispondono ai requisiti di cui al presente regolamento. Laddove siano state rilevate violazioni delle norme di protezione dei dati personali, l'organismo di vigilanza comunica alle autorità di protezione dei dati i risultati delle verifiche.

3. Ove l'organismo di vigilanza imponga al prestatore di servizi fiduciari qualificato di rimediare agli eventuali mancati adempimenti dei requisiti di cui al presente regolamento e ove il prestatore non agisca di conseguenza e, se applicabile, entro un limite di tempo stabilito dall'organismo di vigilanza, quest'ultimo, tenendo conto in particolare della dimensione, della durata e delle conseguenze di tale mancato adempimento, può ritirare la qualifica di tale prestatore o del servizio interessato da esso prestato e informare l'organismo di cui all'articolo 22, paragrafo 3, al fine di aggiornare gli elenchi di fiducia di cui all'articolo 22, paragrafo 1. L'organismo di vigilanza comunica al prestatore di servizi fiduciari qualificato la revoca della sua qualifica o della qualifica del servizio interessato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento per le seguenti norme:

- a) accreditamento degli organismi di valutazione della conformità e per la relazione di valutazione di conformità di cui al paragrafo 1;
- b) regole in materia di audit in base alle quali gli organismi di valutazione effettueranno le loro valutazioni della conformità dei prestatori di servizi fiduciari qualificati di cui al paragrafo 1.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*Articolo 21***Avviamento di un servizio fiduciario qualificato**

1. Qualora i prestatori di servizi fiduciari, privi di qualifica, intendano avviare la prestazione di servizi fiduciari qualificati, trasmettono all'organismo di vigilanza una notifica della loro intenzione insieme a una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità.

2. L'organismo di vigilanza verifica se il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento e, in particolare, i requisiti per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati da essi prestati.

Se conclude che il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al primo comma, l'organismo di vigilanza concede la qualifica al prestatore di servizi fiduciari e ai servizi fiduciari da esso prestati e informa l'organismo di cui all'articolo 22, paragrafo 3, affinché aggiorni gli elenchi di fiducia di cui all'articolo 22, paragrafo 1, non oltre tre mesi dopo la notifica a norma del paragrafo 1 del presente articolo.

Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

3. I prestatori di servizi fiduciari qualificati possono iniziare a prestare il servizio fiduciario qualificato dopo che la qualifica è stata registrata negli elenchi di fiducia di cui all'articolo 22, paragrafo 1.

4. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*Articolo 22***Elenchi di fiducia**

1. Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia, che includono le informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono responsabili, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati.

2. Gli Stati membri istituiscono, mantengono e pubblicano, in modo sicuro, gli elenchi di fiducia di cui al paragrafo 1, firmati o sigillati elettronicamente in una forma adatta al trattamento automatizzato.

3. Gli Stati membri notificano alla Commissione, senza indugio, informazioni sull'organismo responsabile dell'istituzione, del mantenimento e della pubblicazione degli elenchi nazionali di fiducia, precisando dove gli elenchi sono pubblicati, e sui certificati utilizzati per firmare o sigillare tali elenchi di fiducia e le eventuali modifiche apportate.

4. La Commissione rende pubbliche, attraverso un canale sicuro, le informazioni di cui al paragrafo 3 in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

5. Entro il 18 settembre 2015, la Commissione, mediante atti di esecuzione, specifica le informazioni di cui al paragrafo 1 e definisce le specifiche tecniche e i formati per gli elenchi di fiducia applicabili ai fini dei paragrafi da 1 a 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*Articolo 23***Marchio di fiducia UE per i servizi fiduciari qualificati**

1. Dopo la registrazione della qualifica di cui all'articolo 21, paragrafo 2, secondo comma, nell'elenco di fiducia di cui all'articolo 22, paragrafo 1, i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.
2. Quando utilizzano il marchio di fiducia UE per i servizi fiduciari qualificati di cui al paragrafo 1, i prestatori di servizi fiduciari qualificati garantiscono che sul loro sito web sia disponibile un link all'elenco di fiducia pertinente.
3. Entro il 1° luglio 2015 la Commissione, mediante atti di esecuzione, fornisce criteri specifici relativi alla forma e, in particolare, alla presentazione, alla composizione, alla dimensione e al disegno del marchio di fiducia UE per i servizi fiduciari qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*Articolo 24***Requisiti per i prestatori di servizi fiduciari qualificati**

1. Allorché rilascia un certificato qualificato per un servizio fiduciario, un prestatore di servizi fiduciari qualificato verifica, mediante mezzi appropriati e conformemente al diritto nazionale, l'identità e, se del caso, eventuali attributi specifici della persona fisica o giuridica a cui il certificato qualificato è rilasciato.

Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato direttamente o ricorrendo a un terzo conformemente al diritto nazionale:

- a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica; o
- b) a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato è stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisfano i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia «significativo» o «elevato»; o
- c) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato a norma della lettera a) o b); o
- d) mediante altri metodi di identificazione riconosciuti a livello nazionale che forniscono una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica. La garanzia equivalente è confermata da un organismo di valutazione della conformità.

2. Un prestatore di servizi fiduciari qualificato che presta servizi fiduciari qualificati:

- a) informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;
- b) impiega personale e, ove applicabile, subcontraenti dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che hanno ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e applica procedure amministrative e gestionali, che corrispondono a norme europee o internazionali;
- c) riguardo alla responsabilità civile per danni a norma dell'articolo 13, mantiene risorse finanziarie adeguate e/o si procura un'assicurazione di responsabilità civile appropriata, conformemente al diritto nazionale;



- d) prima di avviare una relazione contrattuale informa, in modo chiaro e completo, chiunque intenda utilizzare un servizio fiduciario qualificato dei termini e delle condizioni esatte per l'utilizzo di tale servizio, comprese eventuali limitazioni del suo utilizzo;
- e) utilizza sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi che assicurano;
- f) utilizza sistemi affidabili per memorizzare i dati a esso forniti, in modo verificabile, affinché:
  - i) siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati fanno riferimento;
  - ii) soltanto le persone autorizzate possano effettuare inserimenti e modifiche ai dati memorizzati;
  - iii) l'autenticità dei dati sia verificabile;
- g) adotta misure adeguate contro le falsificazioni e i furti di dati;
- h) registra e mantiene accessibili per un congruo periodo di tempo, anche dopo la cessazione delle attività del prestatore di servizi fiduciari qualificato, tutte le informazioni pertinenti relative a dati rilasciati e ricevuti dal prestatore di servizi fiduciari qualificato, in particolare a fini di produzione di prove nell'ambito di procedimenti giudiziari e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;
- i) dispone di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni verificate dall'organismo di vigilanza a norma dell'articolo 17, paragrafo 4, lettera i);
- j) garantisce il trattamento lecito dei dati personali a norma della direttiva 95/46/CE;
- k) se i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati, istituiscono una banca dati dei certificati aggiornata.

3. Se un prestatore di servizi fiduciari qualificato che rilascia certificati qualificati decide di revocare un certificato, registra tale revoca nella propria banca dati dei certificati e pubblica la situazione di revoca del certificato tempestivamente e, in ogni caso, entro 24 ore dal ricevimento della richiesta. La revoca diventa immediatamente effettiva all'atto della pubblicazione.

4. In considerazione del paragrafo 3, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati trasmettono alle parti facenti affidamento sulla certificazione informazioni sulla situazione di validità o revoca dei certificati qualificati da essi rilasciati. Queste informazioni sono rese disponibili almeno per ogni certificato rilasciato in qualsiasi momento e oltre il periodo di validità del certificato, in modo automatizzato, affidabile, gratuito ed efficiente.

5. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sistemi e prodotti affidabili, che soddisfano i requisiti di cui al paragrafo 2, lettere e) ed f), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati ove i sistemi e i prodotti affidabili adempiano a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

## SEZIONE 4

**Firme elettroniche***Articolo 25***Effetti giuridici delle firme elettroniche**

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

*Articolo 26***Requisiti di una firma elettronica avanzata**

Una firma elettronica avanzata soddisfa i seguenti requisiti:

- a) è connessa unicamente al firmatario;
- b) è idonea a identificare il firmatario;
- c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
- d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

*Articolo 27***Firme elettroniche nei servizi pubblici**

1. Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato di firma elettronica e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
2. Se uno Stato membro richiede una firma elettronica avanzata basata su un certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate basate su un certificato qualificato e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
3. Gli Stati membri non richiedono, per un utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, una firma elettronica dotata di un livello di garanzia di sicurezza più elevato di quello della firma elettronica qualificata.
4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alle firme elettroniche avanzate. Si presume che i requisiti per le firme elettroniche avanzate di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 26, siano rispettati ove una firma elettronica avanzata soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento delle firme elettroniche avanzate o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 28*

##### **Certificati qualificati di firme elettroniche**

1. I certificati qualificati di firme elettroniche soddisfano i requisiti di cui all'allegato I.
2. I certificati qualificati di firme elettroniche non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato I.
3. I certificati qualificati di firme elettroniche possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento delle firme elettroniche qualificate.
4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.
5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:
  - a) in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;
  - b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.
6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di firma elettronica. Si presume che i requisiti di cui all'allegato I siano stati rispettati ove un certificato qualificato di firma elettronica risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 29*

##### **Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata**

1. I dispositivi per la creazione di una firma elettronica qualificata soddisfano i requisiti di cui all'allegato II.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai dispositivi per la creazione di una firma elettronica qualificata. Si presume che i requisiti di cui all'allegato II siano stati rispettati ove un dispositivo per la creazione di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 30*

##### **Certificazione dei dispositivi per la creazione di una firma elettronica qualificata**

1. La conformità dei dispositivi per la creazione di una firma elettronica qualificata con i requisiti stabiliti all'allegato II è certificata da appropriati organismi pubblici o privati designati dagli Stati membri.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dell'organismo pubblico o privato di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.

3. La certificazione di cui al paragrafo 1 si basa su uno dei seguenti elementi:

- a) un processo di valutazione di sicurezza condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici incluse nell'elenco redatto conformemente al secondo comma; o
- b) un processo diverso da quello di cui alla lettera a), a condizione che utilizzi livelli di sicurezza comparabili e che l'organismo pubblico o privato di cui al paragrafo 1 notifichi tale processo alla Commissione. Detto processo può essere utilizzato solo in assenza delle norme di cui alla lettera a) ovvero quando è in corso un processo di valutazione di sicurezza di cui alla lettera a).

La Commissione adotta, mediante atti di esecuzione, un elenco di norme per la valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui alla lettera a). Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 48, paragrafo 2.

4. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 47 riguardo alla fissazione di criteri specifici che gli organismi designati di cui al paragrafo 1 del presente articolo devono soddisfare.

#### *Articolo 31*

##### **Pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati**

1. Gli Stati membri notificano alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la conclusione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica qualificata certificati dagli organismi di cui all'articolo 30, paragrafo 1. Essi notificano inoltre alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la cancellazione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica che non sono più certificati.

2. Sulla base delle informazioni pervenute, la Commissione redige, pubblica e mantiene un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati.

3. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure applicabili ai fini del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 32*

##### **Requisiti per la convalida delle firme elettroniche qualificate**

1. Il processo di convalida di una firma elettronica qualificata conferma la validità di una firma elettronica qualificata purché:

- a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I;
- b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma;
- c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione;

- d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;
  - e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma;
  - f) la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata;
  - g) l'integrità dei dati firmati non sia stata compromessa;
  - h) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma;
2. Il sistema utilizzato per convalidare la firma elettronica qualificata fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consente di rilevare eventuali questioni attinenti alla sicurezza.
3. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alla convalida delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove la convalida delle firme elettroniche qualificate risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### Articolo 33

##### **Servizio di convalida qualificato delle firme elettroniche qualificate**

1. Un servizio di convalida qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che:
- a) fornisce la convalida a norma dell'articolo 32, paragrafo 1; e
  - b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di convalida qualificato di cui al paragrafo 1. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il servizio di convalida di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### Articolo 34

##### **Servizio di conservazione qualificato delle firme elettroniche qualificate**

1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

## SEZIONE 5

**Sigilli elettronici**

## Articolo 35

**Effetti giuridici dei sigilli elettronici**

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.
2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.
3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

## Articolo 36

**Requisiti dei sigilli elettronici avanzati**

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

- a) è connesso unicamente al creatore del sigillo;
- b) è idoneo a identificare il creatore del sigillo;
- c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e
- d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

## Articolo 37

**Sigilli elettronici nei servizi pubblici**

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.
4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati. Si presume che i requisiti per i sigilli elettronici avanzati di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 36 siano rispettati ove un sigillo elettronico avanzato soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.



5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 38*

##### **Certificati qualificati di sigilli elettronici**

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.
2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.
3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.
4. Qualora un certificato qualificato di un sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.
5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea dei certificati qualificati di sigilli elettronici:
  - a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, il certificato perde la sua validità per il periodo della sospensione;
  - b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.
6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

#### *Articolo 39*

##### **Dispositivi per la creazione di un sigillo elettronico qualificato**

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.
2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.
3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

#### *Articolo 40*

##### **Convalida e conservazione dei sigilli elettronici qualificati**

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.

## SEZIONE 6

**Validazione temporale elettronica**

## Articolo 41

**Effetti giuridici della validazione temporale elettronica**

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.
2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.
3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

## Articolo 42

**Requisiti per la validazione temporale elettronica qualificata**

1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:
  - a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;
  - b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e
  - c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

## SEZIONE 7

**Servizi elettronici di recapito certificato**

## Articolo 43

**Effetti giuridici di un servizio elettronico di recapito certificato**

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.
2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

*Articolo 44***Requisiti per i servizi elettronici di recapito certificato qualificati**

1. I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:
  - a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;
  - b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;
  - c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;
  - d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;
  - e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
  - f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di invio e ricezione dei dati. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*SEZIONE 8***Autenticazione dei siti web***Articolo 45***Requisiti per i certificati qualificati di autenticazione di siti web**

1. I certificati qualificati di autenticazione di siti web soddisfano i requisiti di cui all'allegato IV.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di autenticazione di siti web. Si presume che i requisiti di cui all'allegato IV siano stati rispettati ove un certificato qualificato di autenticazione di sito web risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

*CAPO IV***DOCUMENTI ELETTRONICI***Articolo 46***Effetti giuridici dei documenti elettronici**

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

## CAPO V

**DELEGA DI POTERE E DISPOSIZIONI DI ESECUZIONE***Articolo 47***Esercizio della delega**

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
2. Il potere di adottare gli atti delegati di cui all'articolo 30, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 17 settembre 2014.
3. La delega di potere di cui all'articolo 30, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
5. L'atto delegato adottato ai sensi dell'articolo 30, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

*Articolo 48***Procedura di comitato**

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

## CAPO VI

**DISPOSIZIONI FINALI***Articolo 49***Riesame**

La Commissione riesamina l'applicazione del presente regolamento e presenta una relazione in proposito al Parlamento europeo e al Consiglio entro il 1° luglio 2020. La Commissione valuta in particolare se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, compresi l'articolo 6, l'articolo 7, lettera f), e gli articoli 34, 43, 44 e 45, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici.

La relazione di cui al primo comma è corredata, se necessario, di proposte legislative.

Ogni quattro anni dopo la relazione di cui al primo paragrafo la Commissione presenta inoltre al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nella realizzazione degli obiettivi del presente regolamento.

*Articolo 50***Abrogazione**

1. La direttiva 1999/93/CEE è abrogata con effetto dal 1° luglio 2016.
2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento.

*Articolo 51***Disposizioni transitorie**

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento.
2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza.
3. Un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE presenta una relazione di valutazione della conformità all'organismo di vigilanza quanto prima e, comunque, non oltre il 1° luglio 2017. Fino alla presentazione della suddetta relazione di valutazione della conformità e fino a che l'organismo di vigilanza non ne abbia completato la valutazione, il prestatore di servizi di certificazione è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento.
4. Se un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE non presenta una relazione di valutazione della conformità all'organismo di vigilanza entro i termini di cui al paragrafo 3, egli non è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento a decorrere dal 2 luglio 2017.

*Articolo 52***Entrata in vigore**

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.
2. Il presente regolamento si applica a decorrere dal 1° luglio 2016, a eccezione delle seguenti disposizioni:
  - a) articolo 8, paragrafo 3, articolo 9, paragrafo 5, articolo 12, paragrafi da 2 a 9, articolo 17, paragrafo 8, articolo 19, paragrafo 4, articolo 20, paragrafo 4, articolo 21, paragrafo 4, articolo 22, paragrafo 5, articolo 23, paragrafo 3, articolo 24, paragrafo 5, articolo 27, paragrafi 4 e 5, articolo 28, paragrafo 6, articolo 29, paragrafo 2, articolo 30, paragrafi 3 e 4, articolo 31, paragrafo 3, articolo 32, paragrafo 3, articolo 33, paragrafo 2, articolo 34, paragrafo 2, articolo 37, paragrafi 4 e 5, articolo 38, paragrafo 6, articolo 42, paragrafo 2, articolo 44, paragrafo 2, articolo 45, paragrafo 2, articolo 47 e articolo 48, che si applicano dal 17 settembre 2014;
  - b) l'articolo 7, l'articolo 8, paragrafi 1 e 2, gli articoli 9, 10, 11 e l'articolo 12, paragrafo 1, si applicano a decorrere dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8;
  - c) l'articolo 6 si applica a decorrere da tre anni dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8.
3. Quando il regime di identificazione elettronica notificato è compreso nell'elenco pubblicato dalla Commissione ai sensi dell'articolo 9 prima della data di cui al paragrafo 2, lettera c), del presente articolo, il riconoscimento dei mezzi di identificazione elettronica in virtù di tale regime ai sensi dell'articolo 6 ha luogo non oltre 12 mesi dopo la pubblicazione di detto regime ma non prima della data di cui al paragrafo 2, lettera c), del presente articolo.

4. Nonostante il paragrafo 2, lettera c), del presente articolo, uno Stato membro può decidere che i mezzi di identificazione elettronica a norma del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, da un altro Stato membro, siano riconosciuti nel primo Stato membro a decorrere dalla data di pubblicazione degli atti di esecuzione di cui agli articoli 8, paragrafo 3, e 12, paragrafo 8. Gli Stati membri interessati ne informano la Commissione. La Commissione rende pubbliche tali informazioni.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 23 luglio 2014

*Per il Parlamento europeo*

*Il presidente*

M. SCHULZ

*Per il Consiglio*

*Il presidente*

S. GOZI

---

## ALLEGATO I

**REQUISITI PER I CERTIFICATI QUALIFICATI DI FIRMA ELETTRONICA**

I certificati qualificati di firma elettronica contengono:

- a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;
  - b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e
    - per una persona giuridica: il nome e, se del caso, il numero di registrazione quali figurano nei documenti ufficiali,
    - per una persona fisica: il nome della persona;
  - c) è chiaramente indicato almeno il nome del firmatario, o uno pseudonimo, qualora sia usato uno pseudonimo;
  - d) i dati di convalida della firma elettronica che corrispondono ai dati per la creazione di una firma elettronica;
  - e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;
  - f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;
  - g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;
  - h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;
  - i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;
  - j) qualora i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica siano ubicati in un dispositivo per la creazione di una firma elettronica qualificata, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.
-



## ALLEGATO II

**REQUISITI PER I DISPOSITIVI PER LA CREAZIONE DI UNA FIRMA ELETTRONICA QUALIFICATA**

1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:
    - a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;
    - b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;
    - c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;
    - d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.
  2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.
  3. La generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciari qualificato.
  4. Fatto salvo il punto 1, lettera d), i prestatori di servizi fiduciari qualificati che gestiscono dati per la creazione di una firma elettronica per conto del firmatario possono duplicare i dati per la creazione di una firma elettronica solo a fini di back-up, purché rispettino i seguenti requisiti:
    - a) la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;
    - b) il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio.
-

## ALLEGATO III

**REQUISITI PER I CERTIFICATI QUALIFICATI DEI SIGILLI ELETTRONICI**

I certificati qualificati dei sigilli elettronici contengono:

- a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;
- b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e
  - per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,
  - per una persona fisica: il nome della persona;
- c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;
- d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;
- e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;
- f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;
- g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;
- h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;
- i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;
- j) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

---

## ALLEGATO IV

**REQUISITI PER I CERTIFICATI QUALIFICATI DI AUTENTICAZIONE DI SITI WEB**

I certificati qualificati di autenticazione di siti web contengono:

- a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di autenticazione di sito web;
  - b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e
    - per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,
    - per una persona fisica: il nome della persona;
  - c) per le persone fisiche: almeno il nome della persona a cui è stato rilasciato il certificato, o uno pseudonimo. Qualora sia usato uno pseudonimo, ciò è chiaramente indicato;  
  
per le persone giuridiche: almeno il nome della persona giuridica cui è stato rilasciato il certificato e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;
  - d) elementi dell'indirizzo, fra cui almeno la città e lo Stato, della persona fisica o giuridica cui è rilasciato il certificato e, se del caso, quali appaiono nei documenti ufficiali;
  - e) il nome del dominio o dei domini gestiti dalla persona fisica o giuridica cui è rilasciato il certificato;
  - f) l'indicazione dell'inizio e della fine del periodo di validità del certificato;
  - g) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;
  - h) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;
  - i) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera h) è disponibile gratuitamente;
  - j) l'ubicazione dei servizi competenti per lo status di validità del certificato a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato.
-

## DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014

Definizione delle caratteristiche del sistema pubblico per la gestione dell'identita' digitale di cittadini e imprese (SPID), nonche' dei tempi e delle modalita' di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376)

(GU n.285 del 9-12-2014)

### IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale;

Visto, in particolare, l'art. 64 del decreto legislativo n. 82 del 2005, come modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 69 che, «per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilita', e' istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identita' digitale di cittadini e imprese» (SPID) e demanda a un 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, la definizione delle caratteristiche del sistema SPID, nonche' dei tempi e delle modalita' di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle modalita' attraverso cui le imprese possono avvalersi del sistema SPID per la gestione dell'identita' digitale dei propri utenti;

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, e successive modificazioni, con cui e' stata istituita l'Agenzia per l'Italia digitale;

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 e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta Ufficiale dell'Unione Europea - serie L 257 del 28 agosto 2014;

Visto il decreto del Presidente della Repubblica 21 febbraio 2014 con cui l'onorevole dott.ssa Maria Anna Madia e' stato nominata Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2014 con cui al Ministro senza portafoglio onorevole dottoressa Maria Anna Madia e' stato conferito l'incarico per la semplificazione e la pubblica amministrazione;

Visto il decreto del Presidente del Consiglio dei ministri 23 aprile 2014 recante Delega di funzioni al Ministro senza portafoglio onorevole dott.ssa Maria Anna Madia per la semplificazione e la pubblica amministrazione;

Sentito il Garante per la protezione dei dati personali;

Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento

europeo e del Consiglio, del 20 luglio 1998, recepita con legge 21 giugno 1986, n. 317, modificata dal decreto legislativo 23 novembre 2000, n. 427;

Di concerto con il Ministro dell'economia e delle finanze;

Decreta:

Art. 1

#### Definizioni

1. Ai fini del presente decreto si intende per:

- a) Agenzia: l'Agenzia per l'Italia Digitale;
- b) attributi: informazioni o qualita' di un utente utilizzate per rappresentare la sua identita', il suo stato, la sua forma giuridica o altre caratteristiche peculiari;
- c) attributi identificativi: nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonche' il codice fiscale o la partita IVA e gli estremi del documento d'identita' utilizzato ai fini dell'identificazione;
- d) attributi secondari: il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonche' eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni;
- e) attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati;
- f) autenticazione informatica: verifica effettuata dal gestore dell'identita' digitale, su richiesta del fornitore di servizi, della validita' delle credenziali di accesso presentate dall'utente allo stesso gestore, al fine di convalidarne l'identificazione informatica;
- g) codice identificativo: il particolare attributo assegnato dal gestore dell'identita' digitale che consente di individuare univocamente un'identita' digitale nell'ambito dello SPID;
- h) credenziale di accesso: il particolare attributo di cui l'utente si avvale, unitamente al codice identificativo, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi che aderiscono allo SPID;
- i) fornitore di servizi: il fornitore dei servizi della societa' dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identita' digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identita' digitale, non discriminano gli utenti in base al gestore dell'identita' digitale che l'ha fornita;
- l) gestori dell'identita' digitale: le persone giuridiche accreditate allo SPID che, in qualita' di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identita' digitale degli utenti, la distribuzione e l'interoperabilita' delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti;
- m) gestori di attributi qualificati: i soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validita' di attributi qualificati, su richiesta dei fornitori di servizi;
- n) identificazione informatica: l'identificazione di cui all'art. 1, comma 1, lettera u-ter) del decreto legislativo 7 marzo 2005, n.

82 (di seguito «CAD»);

o) identità digitale: la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi;

p) revoca dell'identità digitale: disattivazione definitiva dell'identità digitale;

q) sospensione dell'identità digitale: disattivazione temporanea dell'identità digitale;

r) registrazione: l'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal presente decreto e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura;

s) registro SPID: registro, tenuto dall'Agenzia, accessibile al pubblico, contenente l'elenco dei soggetti abilitati a operare in qualità di gestori dell'identità digitale, di gestori degli attributi qualificati e di fornitori di servizi;

t) servizio qualificato: servizio per la cui erogazione è necessaria l'identificazione informatica dell'utente;

u) SPID: il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98;

v) utente: persona fisica o giuridica, titolare di un'identità digitale SPID, che utilizza i servizi erogati in rete da un fornitore di servizi, previa identificazione informatica.

## Art. 2

### Oggetto e finalità

1. Il presente decreto stabilisce le caratteristiche dello SPID ai sensi dell'art. 64 del CAD, come modificato dall'art. 17-ter del decreto-legge n. 69 del 2013.

2. Ai sensi di tali disposizioni lo SPID consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

## Art. 3

### Soggetti partecipanti allo SPID

1. I soggetti pubblici o privati che partecipano allo SPID sono:

- a) i gestori dell'identità digitale;
- b) i gestori degli attributi qualificati;
- c) i fornitori di servizi;
- d) l'Agenzia;
- e) gli utenti.

2. I soggetti di cui al comma 1, esclusi gli utenti, costituiscono un sistema aperto e cooperante che consente loro di comunicare utilizzando meccanismi di interazione, standard tecnologici e protocolli indicati nel presente decreto e precisati nelle regole tecniche definite dall'Agenzia nell'ambito dei regolamenti di cui all'art. 4.

## Art. 4

### Ruolo dell'Agenzia

1. L'Agenzia cura l'attivazione dello SPID, svolgendo, in particolare, le seguenti attività:

a) gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni. Con i regolamenti di cui al presente articolo sono disciplinate le convenzioni per l'adesione allo SPID da parte dei fornitori di servizi ed è regolato il contributo che i gestori dell'identità digitale accreditati allo SPID riconoscono all'Agenzia, da determinarsi nella misura necessaria alla copertura dei costi sostenuti da quest'ultima;

b) cura l'aggiornamento del registro SPID e vigila sull'operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate;

c) stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità. A tali convenzioni i gestori dell'identità digitale e i gestori degli attributi qualificati sono tenuti ad aderire secondo le modalità indicate nei regolamenti di cui al presente articolo.

2. Entro trenta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le regole tecniche e le modalità attuative per la realizzazione dello SPID.

3. Entro sessanta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le modalità di accreditamento dei soggetti SPID.

4. Entro sessanta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le procedure necessarie a 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.

## Art. 5

### Attributi dell'identità digitale

1. Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alle comunicazioni tra il gestore dell'identità digitale e l'utente.

2. Al momento della richiesta di rilascio dell'identità digitale, l'utente può chiedere che siano registrati ulteriori attributi secondari.

3. L'Agenzia stabilisce, nell'ambito dei regolamenti di cui all'art. 4, le modalità e le regole tecniche con le quali i gestori dell'identità digitale e i gestori degli attributi qualificati curano e rendono disponibile la verifica degli attributi stessi ai fornitori di servizi. Gli attributi qualificati sono verificati dal fornitore di servizi presso il gestore di attributi qualificati.

## Art. 6

### Livelli di sicurezza delle identità digitali

1. Lo SPID è basato su tre livelli di sicurezza di autenticazione informatica:

a) nel primo livello, corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a un fattore, quale la password, secondo quanto previsto dal presente decreto e dai



regolamenti di cui all'art. 4;

b) nel secondo livello, corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'art. 4;

c) nel terzo livello, corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'art. 4.

2. L'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello, nonché i criteri per la valutazione dei sistemi di autenticazione informatica e la loro assegnazione al relativo livello di sicurezza. In tale ambito, i gestori dell'identità digitale rendono pubbliche le decisioni dell'Agenzia con le modalità indicate dalla stessa.

3. I gestori dell'identità digitale garantiscono che l'autenticazione informatica avvenga attraverso software e soluzioni tecniche che non richiedono ai fornitori di servizi di dotarsi di dispositivi, fissi o mobili, proprietari. Sono consentite soluzioni tecniche che prevedono il caricamento del software necessario per effettuare l'autenticazione informatica.

4. I fornitori di servizi non possono discriminare l'accesso ai propri servizi sulla base del gestore di identità che l'ha fornita.

5. I fornitori di servizi scelgono il livello di sicurezza necessario per accedere ai propri servizi.

## Art. 7

### Rilascio delle identità digitali

1. Le identità digitali sono rilasciate, a domanda dell'interessato, dal gestore dell'identità digitale, previa verifica dell'identità del soggetto richiedente e mediante consegna in modalità sicura delle credenziali di accesso. Nell'ambito della propria struttura organizzativa, i gestori delle identità digitali individuano il responsabile delle attività di verifica dell'identità del soggetto richiedente.

2. La verifica dell'identità del soggetto richiedente e la richiesta di adesione avvengono in uno dei seguenti modi:

a) identificazione del soggetto richiedente che sottoscrive il modulo di adesione allo SPID, tramite esibizione a vista di un valido documento d'identità e, nel caso di persone giuridiche, della procura attestante i poteri di rappresentanza;

b) identificazione informatica tramite documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi;

c) identificazione informatica tramite altra identità digitale SPID di livello di sicurezza pari o superiore a quella oggetto della richiesta;

d) acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale;

e) identificazione informatica fornita da sistemi informatici preesistenti all'introduzione dello SPID che risultino aver adottato, a seguito di apposita istruttoria dell'Agenzia, regole di identificazione informatica caratterizzate da livelli di sicurezza

uguali o superiori a quelli definiti nel presente decreto.

3. Con i regolamenti di cui all'art. 4, l'Agenzia definisce le modalita' con le quali la verifica dell'identita' di cui al comma 2 e' effettuata secondo i piu' alti livelli di controllo disponibili, anche in relazione ai livelli di sicurezza di cui all'art. 6.

4. Nei casi di cui alle lettere b), c) ed e) del comma 2 i dati di adesione vengono forniti direttamente, utilizzando i moduli informatici posti a disposizione in rete dal gestore dell'identita' digitale.

5. I gestori dell'identita' digitale, al fine di poter documentare la corretta attribuzione della stessa, conservano per il periodo prescritto dal comma 8, in relazione alle modalita' di identificazione di cui al comma 2, copia per immagine del documento di identita' esibito e del modulo di cui alla lettera a), copia del log della transazione di cui alle lettere b), c) ed e) o il modulo firmato digitalmente di cui alla lettera d), nonche' i documenti e i dati utilizzati per l'associazione e la verifica degli attributi.

6. I gestori dell'identita' digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente utilizzando prioritariamente i servizi convenzionali di cui all'art. 4, comma 1, lettera c).

7. Nei casi in cui le informazioni necessarie per la verifica degli attributi identificativi non siano accessibili tramite i servizi convenzionali di cui al comma 6, i gestori dell'identita' digitale effettuano tali verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, secondo i criteri e le modalita' stabilite dall'Agenzia con i regolamenti di cui all'art. 4, fatto salvo il caso di cui al comma 2, lettera e).

8. I gestori dell'identita' digitale conservano la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identita' digitale. Alla scadenza del predetto termine, i gestori cancellano la suddetta documentazione. Salvo il subentro ai sensi dell'art. 12, il gestore che cessa l'attivita' prima della scadenza del termine di cui al presente comma trasmette la medesima documentazione all'Agenzia, che la conserva fino alla scadenza del suddetto periodo.

9. I dati personali raccolti ai sensi del presente decreto sono trattati e conservati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

## Art. 8

### Gestione delle identita' digitali

1. Fatto salvo il caso in cui l'aggiornamento degli attributi identificativi avvenga in modalita' automatica tramite le convenzioni previste all'art. 4, comma 1, lettera c), gli utenti sono obbligati a informare tempestivamente il gestore dell'identita' digitale di ogni variazione degli attributi previamente comunicati. Il gestore dell'identita' digitale provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite secondo le modalita' di cui all'art. 7, comma 7.

2. Fatti salvi i casi previsti dall'art. 9, l'utente puo' chiedere al gestore dell'identita' digitale, in qualsiasi momento e a titolo gratuito, la sospensione o revoca della propria identita' digitale ovvero la modifica dei propri attributi secondari e delle proprie credenziali di accesso. A tali richieste il gestore dell'identita' digitale provvede tempestivamente. L'Agenzia, con i regolamenti di cui all'art. 4, stabilisce le procedure per consentire agli utenti la rimozione dei dati contenuti nell'identita' digitale.

3. Il gestore dell'identita' digitale revoca l'identita' digitale se riscontra l'inattivita' della stessa per un periodo superiore a

ventiquattro mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica, utilizzando i servizi messi a disposizione dalle convenzioni di cui all'art. 4, comma 1, lettera c), ovvero, laddove l'informazione non sia disponibile in tali ambiti, attivando opportune e documentate verifiche delle informazioni ricevute.

4. Il gestore dell'identita' digitale, su richiesta dell'utente, gli segnala ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari a tale scopo indicato dall'utente stesso, secondo le regole tecniche definite con i regolamenti di cui all'art. 4.

5. I gestori di identita' SPID possono stipulare accordi con pubbliche amministrazioni al fine di importare nel sistema SPID identita' digitali rilasciate dalle pubbliche amministrazioni conformemente a quanto previsto dall'art. 7.

## Art. 9

### Uso illecito delle identita' digitali

1. Nel caso in cui l'utente ritenga, anche a seguito della segnalazione di cui all'art. 8, comma 4, che la propria identita' digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, puo' chiedere, con le modalita' indicate nei regolamenti di cui all'art. 4, la sospensione immediata dell'identita' digitale al gestore della stessa e, se conosciuto, al fornitore di servizi presso il quale essa risulta essere stata utilizzata. Salvo il caso in cui la richiesta sia inviata tramite posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identita' digitale e il fornitore di servizi eventualmente contattato verificano, anche attraverso uno o piu' attributi secondari, la provenienza della richiesta di sospensione da parte del soggetto titolare dell'identita' digitale e forniscono la conferma della ricezione della medesima richiesta.

2. Nel caso previsto dal comma 1, il gestore dell'identita' digitale sospende tempestivamente l'identita' digitale per un periodo massimo di trenta giorni informandone il richiedente. Scaduto tale periodo, l'identita' digitale e' ripristinata o revocata ai sensi del comma 3.

3. Il gestore revoca l'identita' digitale se, nei termini previsti dal comma 2, riceve dall'interessato copia della denuncia presentata all'autorita' giudiziaria per gli stessi fatti su cui e' basata la richiesta di sospensione.

## Art. 10

### Accreditamento dei gestori dell'identita' digitale

1. Le modalita' di richiesta di accreditamento sono definite nei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4, che possono contenere ulteriori criteri per l'accreditamento delle pubbliche amministrazioni.

2. A seguito dell'accoglimento della richiesta, l'Agenzia stipula apposita convenzione secondo lo schema definito nell'ambito dei regolamenti di cui all'art. 4 e dispone l'iscrizione del richiedente nel registro SPID, consultabile in via telematica.

3. Al fine di ottenere l'accreditamento gli interessati devono:

a) avere forma giuridica di societa' di capitali e un capitale sociale non inferiore a cinque milioni di euro;

b) garantire il possesso, da parte dei rappresentanti legali, dei soggetti preposti all'amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilita' richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'art. 26 del decreto legislativo 1° settembre 1993, n. 385;

c) dimostrare la capacita' organizzativa e tecnica necessaria per svolgere l'attivita' di gestione dell'identita' digitale;

d) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi da fornire. In particolare, il personale addetto alla realizzazione e gestione del sistema informatico deve possedere, in relazione alle attivita' da svolgere, la competenza gestionale, l'appropriata conoscenza e padronanza delle procedure operative e di sicurezza, nonche' delle regole tecniche da applicare. Il gestore provvede al periodico aggiornamento professionale del personale;

e) comunicare all'Agenzia i nominativi e il profilo professionale dei soggetti responsabili delle specifiche funzioni individuate nei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4;

f) essere in possesso della certificazione di conformita' del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative, alla norma ISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia;

g) trattare i dati personali nel rispetto del decreto legislativo 30 giugno 2003, n. 196;

h) essere in possesso della certificazione di qualita' ISO 9001, successive modifiche o norme equivalenti.

4. Le lettere a) e b) del comma 3 non si applicano alle pubbliche amministrazioni che chiedono l'accreditamento al fine di svolgere l'attivita' di gestore dell'identita' digitale.

5. L'Agenzia procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la permanenza della sussistenza dei requisiti previsti dal presente decreto. Se, all'esito dei controlli, accerta la mancanza dei requisiti richiesti per l'iscrizione nel registro SPID, decorso il termine fissato per consentire il ripristino degli stessi, l'Agenzia, con provvedimento motivato notificato all'interessato, puo' adottare le azioni previste dall'art. 12.

## Art. 11

### Obblighi dei gestori dell'identita' digitale

1. I gestori dell'identita' digitale, nel rispetto dei regolamenti di cui all'art. 4:

a) utilizzano sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformita' a criteri di sicurezza riconosciuti in ambito europeo o internazionale;

b) adottano adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrita' e la sicurezza nella generazione delle credenziali di accesso;

c) effettuano un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identita' digitale di ciascun utente, procedendo alla sospensione dell'identita' digitale in caso di attivita' sospetta;

d) effettuano, con cadenza almeno annuale, un'analisi dei rischi;

e) definiscono il piano per la sicurezza dei servizi SPID, da trasmettere all'Agenzia, e ne garantiscono l'aggiornamento;

f) allineano le procedure di sicurezza agli standard internazionali, la cui conformita' e' certificata da un terzo abilitato;

g) conducono, con cadenza almeno semestrale, il «Penetration Test»;

h) garantiscono la continuita' operativa dei servizi afferenti allo SPID;

i) effettuano ininterrottamente l'attivita' di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;

l) garantiscono la gestione sicura delle componenti riservate delle identita' digitali degli utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi,

neppure in forma cifrata;

m) garantiscono la disponibilit  delle funzioni, l'applicazione dei modelli architeturali e il rispetto delle disposizioni previste dal presente decreto e dai regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4;

n) si sottopongono, con cadenza almeno biennale, ad una verifica di conformit  alle disposizioni vigenti da parte di un organismo di valutazione accreditato ai sensi del Regolamento CE 765/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008. Inviano all'Agenzia l'esito della verifica, redatto dall'organismo di valutazione in lingua inglese, entro tre giorni lavorativi dalla sua ricezione;

o) informano tempestivamente l'Agenzia e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali, secondo le modalit  individuate nei regolamenti adottati ai sensi dell'art. 4;

p) adeguano i propri sistemi a seguito degli aggiornamenti emanati dall'Agenzia;

q) inviano all'Agenzia, in forma aggregata, i dati da questa richiesti a fini statistici, che potranno essere resi pubblici.

## Art. 12

### Cessazione, subentro, sospensione e revoca dell'attivit  dei gestori dell'identit  digitale

1. Il gestore dell'identit  digitale comunica all'Agenzia e agli utenti a cui ha attribuito l'identit  digitale l'intenzione di cessare la propria attivit  almeno trenta giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessit  di revocare le identit  digitali dallo stesso rilasciate.

2. Il gestore sostitutivo, previo invio all'Agenzia della dichiarazione di accettazione e previa acquisizione del consenso degli utenti, subentra nella gestione delle identit  digitali rilasciate dal gestore cessato e nella conservazione delle informazioni di cui all'art. 7, comma 8.

3. Salvo quanto disposto al comma 2, il gestore dell'identit  digitale che cessa la propria attivit , scaduto il termine del periodo previsto al comma 1, revoca le identit  digitali rilasciate.

4. L'Agenzia, previo accertamento della violazione delle disposizioni di cui al presente decreto e dei regolamenti attuativi adottati ai sensi dell'art. 4, puo' disporre la sospensione dell'attivit  di attribuzione di identit  digitali per un periodo minimo di un mese e massimo di un anno o, nei casi piu' gravi, la revoca dell'accreditamento del gestore dell'identit  digitale.

5. In caso di revoca dell'accreditamento del gestore dell'identit  digitale si applicano le disposizioni relative alle cessazioni di cui al presente articolo.

## Art. 13

### Adesione ed obblighi dei fornitori di servizi

1. I fornitori di servizi possono aderire allo SPID stipulando apposita convenzione con l'Agenzia il cui schema e' definito nell'ambito dei regolamenti attuativi di cui all'art. 4.

2. I fornitori di servizi conservano per ventiquattro mesi le informazioni necessarie a imputare, alle singole identit  digitali, le operazioni effettuate sui propri sistemi tramite SPID.

3. Nel caso in cui i fornitori di servizi rilevino un uso anomalo di un'identit  digitale, informano immediatamente l'Agenzia e il gestore dell'identit  digitale che l'ha rilasciata.

4. I fornitori di servizi trattano i dati personali nel rispetto del decreto legislativo 30 giugno 2003, n. 196. Nell'ambito

dell'informativa di cui all'art. 13 del decreto legislativo n. 196 del 2003, i fornitori di servizi informano l'utente che l'identità digitale e gli eventuali attributi qualificati saranno verificati, rispettivamente, presso i gestori dell'identità digitale e i gestori degli attributi qualificati.

5. I fornitori di servizi, fatto salvo quanto previsto dall'art. 14 per le pubbliche amministrazioni, possono affidare la gestione delle interfacce di autenticazione informatica ai propri servizi in rete ai gestori di identità SPID.

#### Art. 14

##### Adesione allo SPID da parte delle pubbliche amministrazioni in qualità di fornitori di servizi

1. Nel rispetto dell'art. 64, comma 2, del CAD, le pubbliche amministrazioni che erogano in rete servizi qualificati, direttamente o tramite altro fornitore di servizi, consentono l'identificazione informatica degli utenti attraverso l'uso dello SPID.

2. Ai fini del comma 1, le pubbliche amministrazioni di cui all'art. 2, comma 2, del CAD aderiscono allo SPID, secondo le modalità stabilite dall'Agenzia ai sensi dell'art. 4, entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale.

3. Le pubbliche amministrazioni possono affidare ai gestori di identità dello SPID le funzioni di autenticazione informatica previste dalla normativa vigente in materia.

4. Le pubbliche amministrazioni possono affidare ai gestori di identità SPID le funzioni di autenticazione informatica basate sugli strumenti per i quali il diritto dell'Unione europea prevede il mutuo riconoscimento.

5. Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati. Per l'adeguamento allo SPID dei propri sistemi informatici, le amministrazioni utilizzano le risorse finanziarie disponibili a legislazione vigente, senza nuovi e maggiori oneri a carico della finanza pubblica.

#### Art. 15

##### Adesione allo SPID da parte di soggetti privati fornitori di servizi

1. Non possono aderire allo SPID i soggetti privati fornitori di servizi il cui rappresentante legale, soggetto preposto all'amministrazione o componente di organo preposto al controllo risulta condannato con sentenza passata in giudicato per reati commessi a mezzo di sistemi informatici.

2. Ai sensi dell'art. 64, comma 2-quinquies, del CAD, i soggetti privati che aderiscono allo SPID per la verifica dell'accesso ai servizi erogati in rete, nel rispetto del presente decreto e dei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4, soddisfano gli obblighi di cui all'art. 17, comma 2, del decreto legislativo 9 aprile 2003, n. 70 con la comunicazione del codice identificativo dell'identità digitale utilizzata dall'utente.

3. Nella convenzione che i fornitori di servizi privati stipulano con l'Agenzia, nell'ambito dei regolamenti attuativi di cui all'art. 4, possono essere regolati i corrispettivi dovuti dai fornitori di servizi ai gestori dell'identità digitale e ai gestori degli attributi qualificati per i servizi di verifica.

#### Art. 16

##### Accreditamento dei gestori di attributi qualificati

1. I soggetti che hanno il potere, in base alle norme vigenti, di attestare gli attributi qualificati si accreditano indicando i dati che intendono rendere disponibili nello SPID, nel rispetto del presente decreto e secondo le modalita' indicate nei regolamenti attuativi adottati ai sensi dell'art. 4.

2. L'Agenzia inserisce in un apposito registro, accessibile da parte dei fornitori di servizi, le tipologie di dati resi disponibili da ciascun gestore di attributi qualificati.

3. Su richiesta degli interessati, sono accreditati di diritto i seguenti gestori di attributi qualificati:

a) il Ministero dello sviluppo economico in relazione ai dati contenuti nell'indice nazionale degli indirizzi PEC delle imprese e dei professionisti di cui all'art. 6-bis del CAD;

b) i consigli, gli ordini e i collegi delle professioni regolamentate relativamente all'attestazione dell'iscrizione agli albi professionali;

c) le camere di commercio, industria, artigianato e agricoltura per l'attestazione delle cariche e degli incarichi societari iscritti nel registro delle imprese;

d) l'Agenzia in relazione ai dati contenuti nell'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi di cui all'art. 57-bis del CAD.

#### Art. 17

#### Disposizione finale

1. I soggetti interessati a ottenere l'accreditamento allo SPID possono presentare domanda all'Agenzia successivamente all'emanazione dei regolamenti attuativi di cui all'art. 4.

Il presente decreto e' inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 24 ottobre 2014

p. Il Presidente del Consiglio dei ministri  
Il Ministro per la semplificazione  
e la pubblica amministrazione  
Madia

Il Ministro dell'economia  
e delle finanze  
Padoan

Registrato alla Corte dei conti il 24 novembre 2014

Ufficio controllo atti P.C.M. Ministeri giustizia e affari esteri  
Reg.ne - Prev. n. 3020



DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 10 novembre 2014, n. 194

Regolamento recante modalita' di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente. (15G00002)

(GU n.5 del 8-1-2015)

Vigente al: 23-1-2015

IL PRESIDENTE  
DEL CONSIGLIO DEI MINISTRI

Visto l'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, introdotto dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e, in particolare, il comma 6, lettere a) e b) del medesimo articolo 62;

Vista la legge 24 dicembre 1954, n. 1228, recante "Ordinamento delle anagrafi della popolazione residente";

Visto il decreto del Presidente della Repubblica 29 settembre 1973, n. 605, recante "Disposizioni relative all'anagrafe tributaria e al codice fiscale dei contribuenti", e successive modificazioni;

Vista la legge 27 ottobre 1988, n. 470, recante "Anagrafe e censimento degli italiani all'estero";

Visto il decreto del Presidente della Repubblica 30 maggio 1989, n. 223, recante "Approvazione del nuovo regolamento anagrafico della popolazione residente";

Visto il decreto legislativo 6 settembre 1989, n. 322, recante "Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400";

Visto il decreto del Presidente della Repubblica 6 settembre 1989, n. 323, recante "Regolamento per l'esecuzione della legge 27 ottobre 1988, n. 470, sull'anagrafe e il censimento degli italiani all'estero";

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421", e successive modificazioni, e, in particolare, l'articolo 3;

Visto il decreto del Presidente della Repubblica 3 novembre 2000, n. 396, recante "Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile";

Visto il decreto legislativo del 30 marzo 2001, n. 165, recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";

Visto il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali", e successive modificazioni;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", e successive modificazioni;

Visto il Regolamento (CE) n. 862/2007 del Parlamento europeo e del

Consiglio dell'11 luglio 2007 relativo alle statistiche comunitarie in materia di migrazione e di protezione internazionale;

Visto il Regolamento (CE) n. 763/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 relativo ai censimenti della popolazione e delle abitazioni;

Visto il Regolamento (CE) n. 1201/2009 della Commissione del 30 novembre 2009 recante attuazione del Regolamento (CE) n. 763/2008 del Parlamento europeo e del Consiglio, per quanto riguarda le specifiche tecniche delle variabili e delle loro classificazioni;

Visti il Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio e, in particolare, l'articolo 13 che disciplina il Programma Statistico europeo, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il Regolamento (CE) n. 322/1997 del Consiglio, relativo alle statistiche comunitarie, e la Decisione 89/382/CEE, Euratom del Consiglio che istituisce un comitato del programma statistico delle Comunità europee;

Visto il Regolamento (UE) n. 1260/2013 del Parlamento europeo e del Consiglio del 20 novembre 2013 relativo alle statistiche demografiche europee;

Visto il decreto del Presidente della Repubblica 7 settembre 2010, n. 166, recante "Approvazione del Regolamento recante il riordino dell'Istituto nazionale di statistica" e, in particolare, l'articolo 2, comma 2, lettera c)";

Visto l'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilità 2013)", e successive modificazioni;

Visto il decreto del Presidente del Consiglio dei ministri 23 agosto 2013, n. 109, recante "Disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR)";

Visto il decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari";

Sentito l'Istituto Nazionale di Statistica, che si è espresso con pareri del 26 febbraio 2014 e del 12 giugno 2014;

Acquisito il parere del Garante per la protezione dei dati personali, che si è espresso con nota in data 17 aprile 2014;

Acquisita l'intesa con l'Agenzia per l'Italia digitale;

Acquisita l'intesa con la Conferenza unificata nella seduta del 5 agosto 2014;

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, e successive modificazioni;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 25 settembre 2014;

Su proposta del Ministero dell'interno, del Ministro per la semplificazione e la pubblica amministrazione, di concerto con il Ministro dell'economia e delle finanze;

Adotta

il seguente regolamento:

Art. 1

Subentro alle anagrafi tenute dai comuni

1. L'Anagrafe Nazionale della Popolazione Residente (ANPR) subentra

gradualmente alle anagrafi tenute dai comuni secondo il piano di subentro e le modalita', idonee a garantire l'integrita', l'univocita' e la sicurezza dei dati, descritti nell'Allegato A, che costituisce parte integrante del presente regolamento. Nel subentro sono compresi i dati informatizzati relativi alle situazioni anagrafiche pregresse alla data del subentro e alle schede archiviate in formato elettronico.

2. I dati anagrafici inviati dai comuni ai fini del subentro sono sottoposti ai seguenti controlli formali da parte del Ministero dell'interno:

a) validazione del codice fiscale previo confronto con l'anagrafe tributaria, di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605;

b) verifica di congruita' con i dati contenuti nell'ANPR al momento del subentro.

3. Il Ministero dell'Interno e l'Istituto nazionale di statistica, sentito il Garante per la protezione dei dati personali, definiscono standard e indicatori finalizzati a monitorare la qualita' dei dati registrati nell'ANPR nella fase di subentro.

4. L'ANPR rende disponibile ai comuni, a seguito del subentro, i dati necessari all'allineamento delle banche dati eventualmente conservate dagli stessi.

## Art. 2

### Dati contenuti nell'ANPR e modalita' di conservazione

1. Nell'ANPR sono contenuti i dati del cittadino, della famiglia anagrafica e della convivenza di cui agli articoli 20, 21 e 22 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, e successive modificazioni, i dati dei cittadini italiani residenti all'estero, registrati dai Comuni ai sensi del decreto del Presidente della Repubblica 6 settembre 1989, n. 323, nonche' il domicilio digitale, di cui all'articolo 3-bis, del decreto legislativo 7 marzo 2005, n. 82.

2. I campi relativi ai dati di cui al comma 1 sono descritti nell'Allegato B, che costituisce parte integrante del presente regolamento.

3. L'ANPR conserva le variazioni anagrafiche e i dati relativi alle situazioni anagrafiche pregresse.

4. L'ANPR conserva, in una distinta sezione, le schede anagrafiche relative alle persone cancellate.

## Art. 3

### Garanzie e misure di sicurezza nel trattamento dei dati personali

1. I dati contenuti nell'ANPR sono trattati secondo le modalita' e le misure di sicurezza per la protezione dei dati descritte nell'Allegato C, che costituisce parte integrante del presente regolamento, adottate nel quadro delle piu' ampie misure di cui agli articoli da 31 a 36 e all'allegato B del decreto legislativo 30 giugno 2003, n. 196.

2. Titolare del trattamento dei dati contenuti nell'ANPR, ai sensi dell'articolo 4, comma 1, lettera a), del citato decreto legislativo n. 196 del 2003, e' il Ministero dell'interno, il quale provvede alla conservazione, alla comunicazione dei dati, nonche' all'adozione delle misure di sicurezza di cui al comma 1.

3. Il sindaco, nell'esercizio delle attribuzioni di cui all'articolo 54 del decreto legislativo 18 agosto 2000, n. 267, e successive modificazioni, e' titolare del trattamento dei dati di propria competenza, limitatamente alla registrazione dei dati stessi.

4. La societa' di cui all'articolo 1, comma 306, della legge 24

dicembre 2012, n. 228, e' designata responsabile del trattamento dei dati dal Ministero dell'Interno ai sensi dell'articolo 29 del decreto legislativo n. 196, del 2003.

#### Art. 4

##### Servizi resi disponibili dall'ANPR ai Comuni

1. L'ANPR rende disponibili ai Comuni per i quali e' completato il subentro di cui all'articolo 1, i servizi descritti nell'Allegato D, che costituisce parte integrante del presente regolamento, secondo le modalita' indicate nell'Allegato C.

#### Art. 5

##### Servizi resi disponibili dall'ANPR alle pubbliche amministrazioni

1. Le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, e gli organismi che erogano pubblici servizi, fruiscono dei servizi di cui all'Allegato D, per l'espletamento dei propri compiti istituzionali, secondo le modalita' indicate nell'Allegato C.

2. L'ANPR rende disponibili all'Istituto nazionale di statistica, mediante i servizi previsti nell'Allegato D, i dati di cui all'articolo 2, concernenti la popolazione, il movimento naturale e i trasferimenti di residenza, necessari alla produzione delle statistiche ufficiali sulla popolazione e sulla dinamica demografica, nel rispetto della normativa nazionale e della legislazione dell'Unione Europea.

3. Il Ministero dell'interno - Direzione Centrale per i Servizi Demografici verifica i presupposti e le condizioni di legittimita' dell'accesso ai servizi di cui al presente articolo.

4. Il comune, anche mediante le convenzioni previste dall'articolo 62, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, consente la fruizione dei dati anagrafici della popolazione residente nel proprio territorio, con riguardo altresì agli elenchi di cui all'articolo 34 del decreto del Presidente della Repubblica n. 223 del 1989. La verifica dei presupposti e delle condizioni di legittimita' dell'accesso ai dati e' svolta dal sindaco.

#### Art. 6

##### Accesso all'ANPR da parte del cittadino

1. Il cittadino registrato nell'ANPR puo' esercitare il diritto di accesso ai propri dati personali e gli altri diritti di cui all'articolo 7 del decreto legislativo n. 196 del 2003 presso gli uffici anagrafici, anche consolari, ovvero tramite sito web dell'ANPR, in modalita' diretta e sicura, e previa identificazione informatica ai sensi dell'articolo 64 del citato decreto legislativo n. 82 del 2005 e trasmissione dei dati in modalita' protetta.

#### Art. 7

##### Clausola di invarianza finanziaria

1. Ai fini dell'attuazione delle disposizioni del presente regolamento si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il presente decreto sara' trasmesso alla Corte dei conti per la registrazione.

Il presente decreto, munito di sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 10 novembre 2014

Il Presidente  
del Consiglio dei ministri  
Renzi

Il Ministro dell'interno  
Alfano

Il Ministro per la semplificazione  
e la pubblica amministrazione  
Madia

Il Ministro dell'economia  
e delle finanze  
Padoan

Visto, il Guardasigilli: Orlando

Registrato alla Corte dei conti il 18 dicembre 2014  
Ufficio controllo atti P.C.M. Ministeri giustizia e affari esteri,  
Reg.ne - Prev. n. 3258

Allegato A

Piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni e modalità di subentro

A) Piano per il graduale subentro.

Il Piano per il graduale subentro (nel seguito "Piano") riguarda la progressiva migrazione delle basi dati comunali (APR ed AIRE) verso la base dati centrale ANPR.

Al fine di garantire la predisposizione della base di dati da utilizzare per la migrazione dei Comuni, l'ANPR è preliminarmente popolata con i dati presenti nelle partizioni della stessa, corrispondenti ai sistemi informativi INA e AIRE, attualmente ubicate presso il Centro Nazionale dei Servizi (CNSD) e i Servizi Informativi e Elettorali (SIE) del Ministero dell'Interno.

Tale popolamento iniziale anticipa la fase di validazione dei dati che contribuiscono alla determinazione del codice fiscale (cognome e nome; sesso; luogo e data di nascita), previo confronto con l'anagrafe tributaria di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605 e la verifica di congruità a livello nazionale.

Il Comune riceverà la segnalazione di eventuali anomalie rilevate che dovrà rimuovere utilizzando le proprie applicazioni e provvedendo ad un nuovo invio dei dati con le modalità attualmente previste nell'ambito dei sistemi INA ed AIRE.

Il Piano individua su base mensile, a decorrere dal completamento di tale popolamento iniziale, i comuni che avviano la migrazione delle proprie banche dati APR ed AIRE locali verso l'ANPR, previo assolvimento dell'obbligo di revisione di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223.

I comuni sono individuati sulla base di criteri di distribuzione geografica e di dimensione demografica, descritti nel seguito, assicurando un popolamento medio mensile di 8.000.000 di soggetti residenti, per dieci periodi della durata di 30 giorni ciascuno.

La pianificazione e' cadenzata per settimane, secondo il piano seguente.

Settimana dalla 1 alla 20: comuni con popolazione fino a 100.000 abitanti, individuati, per ciascuna settimana, secondo i criteri di distribuzione geografica e dimensione demografica, espressi dai seguenti valori percentuali:

Distribuzione geografica	Dimensione demografica
Nord: 56 %	fino a 5.000 abitanti: 70 %
Centro: 12 %	tra 5.001 e 20.000 abitanti: 24 %
Sud e isole: 32 %	tra 20.001 e 100.000 abitanti: 6 %

Settimana dalla 21 alla 24: comuni con popolazione compresa tra 100.001 e 200.000 abitanti, individuati, per ciascuna settimana, secondo il criterio di distribuzione geografica e degli ulteriori criteri riferiti al grado di informatizzazione e all'uniformita' dei sistemi informativi.

Settimana dalla 25 alla 32: comuni di citta' metropolitane, individuati, per ciascuna settimana, secondo criteri riferiti al grado di informatizzazione e all'uniformita' dei sistemi informativi.

La durata delle procedure di subentro per ogni comune e' stimata in due settimane, di cui la prima e' dedicata agli invii e la seconda al completamento delle elaborazioni.

Il comune trasmette i dati relativi alle posizioni informatizzate anagrafiche pregresse e alle schede archiviate alla data di inizio del subentro, dopo il completamento dell'invio dei dati relativi alla popolazione residente.

B) Modalita' di subentro.

Il Piano di subentro e' pubblicato sul sito del Ministero dell'interno, Direzione Centrale per i Servizi Demografici, entro trenta giorni dalla pubblicazione del presente decreto nella Gazzetta Ufficiale della Repubblica Italiana.

Sono pubblicati:

l'elenco dei Comuni che dovranno migrare le proprie banche dati (APR), con indicazione della data in cui, per ciascun Comune, e' previsto l'avvio delle operazioni di subentro. L'elenco e' reso disponibile con congruo anticipo rispetto all'avvio delle suddette operazioni e puo' essere oggetto di aggiornamento con cadenza mensile;

le specifiche tecniche e le relative modalita' per l'utilizzo dei servizi di cui all'allegato D, compresi quelli che i Comuni devono utilizzare per inviare i dati contenuti nelle proprie APR, nonche' le relative modalita' di invio. Tali informazioni sono rese disponibili almeno centoventi giorni prima dell'avvio operativo del Piano di subentro.

I dati inviati dai comuni al fine del subentro sono sottoposti ai seguenti controlli formali:

a) verifica di conformita' del messaggio allo standard definito dal Ministero dell'Interno e pubblicato nel sito WEB di ANPR;

b) validazione del codice fiscale previo confronto con l'anagrafe tributaria, di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605;

c) verifica di congruita' con i dati contenuti nell'ANPR al momento del subentro.

Il sistema segnala al comune le anomalie relative al codice fiscale e le altre eventuali anomalie ed incongruenze mediante un apposito messaggio.

Il sistema invia al comune, via posta elettronica certificata, un apposito messaggio di conferma del subentro con indicazione di data e ora.

Il comune risolve le anomalie e le incongruenze segnalate entro trenta giorni, utilizzando i servizi di registrazione dati di cui all'allegato D.

## ALLEGATO B

### CAMPI RELATIVI AI DATI CONTENUTI NELL'ANPR

#### A) SCHEDA INDIVIDUALE DELLA POPOLAZIONE RESIDENTE IN ITALIA

- Codice comunale  
identificativo di individuo
- Codice fiscale
- Comune
- Cognome
- Nome
- Paternita'
- Maternita'
- Luogo Nascita
- Atto Nascita
- Data Nascita
- Sesso
- Stato Civile
- Cognome Coniuge
- Nome Coniuge
- Data matrimonio
- Luogo matrimonio
- Atto matrimonio
- Ordine del matrimonio  
precedente la vedovanza
- Data sentenza divorzio
- Numero sentenza divorzio
- Ordine del matrimonio  
precedente il divorzio
- Cittadinanza
- Data prima iscrizione
- Motivo iscrizione
- Numero pratica
- Data perfezionamento pratica
- Data decorrenza indirizzo
- Specie indirizzo
- Codice identificativo di  
toponimo
- Denominazione indirizzo
- Numero civico (N)
- Scala o corte
- Interno
- Numero isolato
- Domicilio digitale
- Indirizzo estero
- Motivo Cancellazione  
/Reiscrizione
- Descrizione Motivo

Cancellazione /Reiscrizione

- Data Cancellazione/

Reiscrizione

- Motivo Mutazione
- Descrizione Motivo

Mutazione

- Data Mutazione
- Numero pratica
- Data perfezionamento pratica
- Data morte
- Luogo morte
- Atto di morte
- Anno censimento
- Sezione censimento
- Numero foglio censimento
- Numero Carta d'Identita'
- Data Rilascio Carta d'Identita'
- Estremi del permesso di soggiorno
- Lista elettorale
- Lista di leva
- Titolo di studio
- Posizione nella professione/condizione non professionale

## B) SCHEDA DI FAMIGLIA DEI RESIDENTI IN ITALIA

Comune

Provincia

Data costituzione

Motivo costituzione

Data eliminazione

Motivo eliminazione

Intestatario famiglia

Data intestatario famiglia

Cognome tutore intestatario  
minorenne

Nome tutore intestatario minorenne

Data decorrenza indirizzo

Specie indirizzo

Denominazione indirizzo

Numero civico (N)

Scala o corte

Interno

Numero isolato

Frazione

Anno censimento

Sezione censimento

Numero foglio censimento

Numero di componenti minorenni  
presenti nella scheda di famiglia

Per ogni familiare:

Progressivo d'ordine

Relazione di parentela

Cognome

Nome

Sesso

Paternita'

Maternita'

Luogo Nascita

Data Nascita

Atto Nascita



Stato Civile  
Cittadinanza  
Data matrimonio  
Luogo matrimonio  
Cognome Coniuge  
Nome Coniuge  
Atto matrimonio  
Data morte coniuge  
Luogo morte coniuge  
Atto morte coniuge  
Data sentenza divorzio  
Numero sentenza divorzio  
Professione/condizione non  
professionale  
Anno censimento  
Sezione censimento  
Numero foglio censimento

C) SCHEDA DI CONVIVENZA DEI RESIDENTI IN ITALIA

Comune  
Provincia  
Specie della convivenza  
Denominazione della convivenza  
Responsabile della convivenza  
Data responsabile convivenza  
Data decorrenza indirizzo  
Specie indirizzo  
Denominazione indirizzo  
Numero civico (N)  
Scala o corte  
Interno  
Numero isolato  
Frazione  
Anno censimento  
Sezione censimento  
Numero foglio censimento  
Per ogni convivente:  
Progressivo d'ordine convivenza  
Cognome  
Nome  
Sesso  
Paternita'

Maternita'  
Luogo Nascita  
Data Nascita  
Atto Nascita  
Stato Civile  
Cittadinanza  
Data matrimonio  
Luogo matrimonio  
Cognome Coniuge  
Nome Coniuge  
Atto matrimonio  
Data morte coniuge  
Luogo morte coniuge  
Atto morte coniuge  
Data sentenza divorzio  
Numero sentenza divorzio  
Professione/condizione non  
professionale  
Anno censimento  
Sezione censimento

Numero foglio censimento

D) SCHEDA DEI CITTADINI ITALIANI RESIDENTI ALL'ESTERO

codice famiglia  
codice territorio estero di residenza  
codice consolato di residenza  
provincia/contea  
c.a.p.  
localita'  
indirizzo  
numero civico  
presso  
cognome  
nome  
data nascita  
codice iscrizione  
comune nascita  
luogo nascita  
territorio estero nascita  
stato civile  
codice sesso  
codice relazione parentela  
comune iscrizione  
data iscrizione  
motivo iscrizione  
iniziativa iscrizione  
iniziativa aggiornamento  
individuazione comune di iscrizione  
comune di provenienza  
territorio estero di provenienza  
cognome coniuge  
data arrivo nel consolato  
anno espatrio  
comune estremi nascita  
anno estremi nascita  
serie estremi nascita  
parte estremi nascita  
numero estremi nascita  
data stato civile  
comune stato civile  
territorio estero stato civile  
luogo stato civile  
comune registrazione stato civile  
anno registrazione stato civile  
serie registrazione stato civile  
parte registrazione stato civile  
numero registrazione stato civile  
titolo di studio  
attualmente disoccupato  
posizione professionale  
settore di attivita'  
codice fiscale  
tipo elettore  
data inizio istruttoria  
data fine istruttoria  
flag stato istruttoria  
documenti espatrio  
note

E) ULTERIORI CAMPI RELATIVI A DATI DI SERVIZIO

Nell'ANPR sono altresì contenuti gli ulteriori campi relativi ai

dati di servizio necessari a garantire l'interoperabilita' con le banche dati di rilevanza nazionale e regionale, nonche' con le banche dati comunali, ai fini dell'esercizio delle funzioni di competenza.

## Allegato C

### Misure di sicurezza

Il presente allegato descrive le caratteristiche della piattaforma e le misure adottate per garantire l'integrita' e la riservatezza dei dati scambiati e conservati, la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate, in conformita' agli articoli 64, comma 2 e 65, comma 1, lettera c), del decreto legislativo 7 marzo 2005, n. 82.

Per le predette finalita', l'ANPR e' dotata di:

- un sistema di Identity & Access Management per l'identificazione dell'utente e della postazione, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni;

- un sistema di tracciamento e di conservazione dei dati di accesso alle componenti applicative e di sistema;

- sistemi di sicurezza per la protezione delle informazioni e dei servizi erogati dalla base dati;

- un sistema di log analysis per l'analisi periodica dei file di log, in grado di individuare, sulla base di regole predefinite e formalizzate eventi potenzialmente anomali e di segnalarli al Ministero dell'interno tramite funzionalita' di alert;

- una Certification Authority;

- sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni;

- sistemi e servizi di Disaster Recovery.

Il piano di continuita' operativa di cui all'articolo 50-bis del decreto legislativo 7 marzo 2005, n. 82, esplicitera' le procedure relative ai sistemi ed ai servizi di backup e di Disaster Recovery.

#### 1. Infrastruttura fisica

L'infrastruttura di ANPR e' installata nella sede della Societa' di cui all'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228 (nel seguito "la Societa'") ed e' gestita dalla Societa' stessa.

I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi necessari a garantire la continuita' operativa del sistema.

Qualsiasi altra operazione manuale e' consentita solo a personale autorizzato dal Ministero dell'interno.

La suddetta infrastruttura, oltre alle componenti di sicurezza, comprende i sistemi e le basi dati di cui al punto 4.1 dell'allegato al decreto del Presidente del Consiglio di Ministri 23 agosto 2013, n. 109.

#### 2. Accesso alla base dati

L'accesso nell'ANPR avviene in condizioni di pieno isolamento operativo e di esclusivita', in conformita' ai principi di esattezza, disponibilita', accessibilita', integrita' e riservatezza dei dati, dei sistemi e delle infrastrutture, di cui all'articolo 51 del decreto legislativo n. 82 del 2005.

I sistemi di sicurezza garantiscono che l'infrastruttura di produzione sia logicamente distinta dalle altre infrastrutture della Societa' e che l'accesso alla stessa avvenga in modo sicuro, controllato, e costantemente tracciato, esclusivamente da parte di personale autorizzato dal Ministero dell'interno, e con il tracciamento degli accessi e di qualsiasi attivita' eseguita.

L'ANPR invia e riceve le comunicazioni in modalita' sicura, su rete di comunicazione SPC ovvero, tramite Internet, mediante protocollo SSL per garantire la riservatezza dei dati su reti pubbliche.

Le modalita' di accesso da parte dei comuni, delle pubbliche

amministrazioni e degli organismi che erogano pubblici servizi si applicano fino alla piena attuazione delle disposizioni di cui all'articolo 64 del decreto legislativo n. 82 del 2005.

## 2.1 Accesso dei comuni

L'accesso dei comuni all'ANPR avviene tramite sito web o mediante web service.

Accesso del comune tramite sito web dell'ANPR.

I requisiti di sicurezza prevedono il riconoscimento dell'operatore e della postazione, autorizzata dal comune, e dotata dei seguenti dispositivi:

- certificato identificativo, riferito alla postazione, memorizzato al suo interno, emesso dalla Certification Authority;

- smart-card dedicata e personale, e relativo lettore, con certificato client di autenticazione, intestato all'operatore, emesso dalla Certification Authority.

L'infrastruttura di Identity & Access Management garantisce l'autenticazione dell'utente e la verifica dei diritti di accesso dello stesso alle varie risorse, in base al relativo profilo autorizzativo.

L'operatore accede dalla postazione certificata autenticandosi tramite certificato client.

La postazione e' identificata mediante la connessione del browser dell'utente a un indirizzo gestito da un apparato di sicurezza specializzato, che verifica la validita' del certificato identificativo della postazione e, in caso di esito positivo, la validita' del certificato client.

Il sistema di Identity & Access management autorizza l'utente in base al profilo assegnato ed effettua i controlli formali sui messaggi ricevuti.

Il sistema di tracciamento conserva le informazioni relative alla associazione utente - postazione - dati acceduti, inclusi i riferimenti temporali.

Tutte le informazioni relative al tracciamento dei dati sono accessibili solo dagli incaricati autorizzati su specifica richiesta da parte degli organi competenti.

Tutte le operazioni effettuate sono tracciate e conservate.

Accesso del comune mediante web service.

I requisiti di sicurezza prevedono:

- il certificato identificativo, riferito alla postazione, memorizzato al suo interno, emesso dalla Certification Authority;

- il riconoscimento dell'operatore tramite la userid e password utilizzata per accedere ai servizi dei sistemi informativi comunali, che garantiscono l'autenticazione dell'utente e la verifica dei diritti di accesso dello stesso alle varie funzionalita' applicative;

- il certificato identificativo, riferito al server ospitante l'applicazione che utilizza il web service, memorizzato al suo interno, emesso dalla Certification Authority.

L'operatore accede autenticandosi tramite la userid e la password utilizzata per accedere ai servizi dei sistemi informativi comunali.

Per garantire il riconoscimento dell'operatore e della postazione, autorizzata dal comune, nonche' l'integrita' dei dati, i messaggi inviati prevedono:

- identificativo postazione firmato con il certificato di postazione;

- identificativo utente;

- firma dell'intero messaggio mediante il certificato che identifica il server comune secondo i meccanismi standard della ws security.

Alla ricezione del messaggio, ANPR verifica la firma del messaggio ed il sistema di Identity & Access management verifica la validita' dell'identificativo della postazione, nonche' l'esistenza dell'utente e la rispondenza dell'operazione richiesta in base al profilo assegnato; in caso di esito positivo, ANPR elabora il messaggio.

Il sistema di tracciamento conserva le informazioni relative

all'associazione utente - postazione - dati acceduti, inclusi i riferimenti temporali.

Tutte le informazioni relative al tracciamento dei dati sono accessibili solo dagli incaricati autorizzati su specifica richiesta da parte degli organi competenti.

Tutte le operazioni effettuate sono tracciate e conservate.

Il comune garantisce l'adeguamento delle applicazioni alle regole di sicurezza descritte.

#### 2.1.1 Registrazione degli utenti ed assegnazione degli strumenti di sicurezza

L'infrastruttura di Identity e Access Management censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione delle credenziali, secondo la seguente procedura:

a) il sindaco o suo delegato individua gli operatori comunali preposti all'accesso all'ANPR e ne comunica i nominativi al Ministero dell'interno, evidenziando gli operatori che saranno titolari di smart-card;

b) sulla base della comunicazione di cui al punto a), la società registra nel sistema di Identity e Access Management gli operatori comunali ed emette le smart-card richieste, e le trasmette alle Prefetture;

c) la società predispone i plichi che contengono i PIN/PUK e li trasmette ai comuni;

d) le Prefetture consegnano al sindaco le smart-card;

e) il sindaco individua l'Amministratore locale della sicurezza e, tramite la propria smart-card personale ed una specifica applicazione, registra le generalità della persona individuata, gli consegna la smart card e il plico con i PIN/PUK, associa alla persona il ruolo di Amministratore locale della sicurezza, in possesso delle autorizzazioni descritte di seguito;

f) il sindaco comunica al Ministero dell'interno il nominativo dell'Amministratore locale della sicurezza, assicurando l'avvenuta consegna dei dispositivi;

g) l'Amministratore locale della sicurezza accede con la propria smart-card ad un'apposita applicazione dedicata alla gestione degli operatori comunali, consegna le smart-card e le relative buste con i PIN/PUK a ciascuno dei soggetti indicati dal sindaco ai sensi della lettera a), assegna i profili per l'accesso alle applicazioni, revoca le autorizzazioni, blocca le smart-card, richiede nuove smart-card in caso di impossibilità di utilizzo di quella assegnata, registra nuovi operatori comunali, prenotando contestualmente la relativa smart-card che sarà successivamente recapitata dalla società, con modalità analoghe a quelle descritte al punto d);

h) il sindaco accede alla stessa applicazione, può effettuare tutte le operazioni previste per l'Amministratore locale della sicurezza nonché la revoca delle autorizzazioni.

Tutte le funzionalità di sicurezza descritte ai punti precedenti sono disponibili all'interno di un'apposita Web application, cui si accede con autenticazione forte e canale sicuro: la smart-card, pertanto, deve essere necessariamente richiesta per l'Amministratore locale della sicurezza, oltre che per gli operatori comunali che avranno accesso al sito Web di ANPR.

Tramite la suddetta applicazione sono distribuiti i certificati che saranno utilizzati per il riconoscimento delle postazioni.

La gestione e la conservazione della smart-card è di esclusiva responsabilità dell'operatore cui è assegnata, mentre la gestione e la conservazione del certificato che identifica la postazione, memorizzato internamente ad essa, è di responsabilità di un dipendente del Comune appositamente individuato quale responsabile del certificato stesso. La non esportabilità di questo certificato dalla postazione è garantita dalla presenza di un codice PIN, generato in fase di installazione sulla specifica postazione destinataria, la cui conservazione è di esclusiva responsabilità del suddetto dipendente.

Per la gestione dei processi autorizzativi, sono previsti i seguenti ruoli amministrativi, suddivisi tra gli attori del sistema:

- a) Amministratore di Infrastruttura;
- b) Amministratore Applicativo;
- c) Amministratore Centrale della Sicurezza;
- d) Amministratori locali;
- e) Amministratore di primo livello (Sindaco o suo delegato);
- f) Amministratore di secondo livello (Amministratore locale della sicurezza);
- g) Amministratore della postazione (responsabile dei certificati di postazione).

I primi due ruoli sono attribuiti a personale della Società dalla stessa individuato e comunicato al Ministero dell'interno.

Il terzo ruolo è attribuito al personale del Ministero dell'interno.

## 2.2 Accesso delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi

L'accesso delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi all'ANPR avviene tramite sito web o mediante web service.

Per l'accesso tramite sito web, i requisiti di sicurezza prevedono il riconoscimento dell'operatore e della postazione, autorizzata dalla pubblica amministrazione o dall'ente, sulla base del Sistema di Identità Federata, (che contempla anche l'identificativo dell'operatore e l'indirizzo IP della postazione), che consente il controllo degli accessi ai soli servizi di consultazione ed estrazione.

Nel modello di sicurezza dell'Identità Federata, nell'ambito dell'Access & Facility Management, alle pubbliche amministrazioni e agli enti che erogano pubblici servizi sono demandate le funzioni di autenticazione e di autorizzazione, all'interno di profili prestabiliti, assumendo rispettivamente i ruoli di Identity Provider e Attribute Authority, in conformità al modello GFID dell'Agenzia per l'Italia Digitale e mediante l'adozione di soluzioni tecnologiche che garantiscano il tracciamento sia dell'Identity Provider sia dell'operatore.

Le operazioni effettuate presso la postazione sono registrate nel sistema di Identity e Access Management, che registra le informazioni di autenticazione e gli attributi e li utilizza per verificare i diritti di accesso all'informazione e per alimentare il sistema di tracciamento.

Per l'accesso tramite web service, si utilizzano i meccanismi propri del pattern di sicurezza che consente, ove richiesto, di trasferire, ai fini del tracciamento, oltre all'identificativo dell'ente anche l'identificativo dell'utente finale e l'indirizzo IP della sua postazione. Il server applicativo viene identificato tramite apposito certificato.

## 3. Sistema di monitoraggio dei servizi

Il Ministero dell'interno, attraverso l'infrastruttura di cui al paragrafo 1, eroga i servizi di cui all'allegato D e assolve le funzioni di sicurezza descritte nel presente allegato, nel rispetto delle specifiche tecniche elaborate dalla Società e approvate dal Ministero.

Per il monitoraggio dei servizi, il Ministero dell'interno si avvale di uno specifico sistema, ubicato nel Centro Nazionale per i Servizi Demografici del Ministero dell'interno (CNSD), presso il quale sono installate apposite consolle di controllo, utilizzate esclusivamente da personale autorizzato dal Ministero dell'interno per l'accesso in sola visualizzazione.

La visualizzazione completa dello stato del servizio e dell'infrastruttura tecnologica che lo supporta avviene mediante:

a) vista c.d. "ad albero" dei servizi che rendono disponibili le seguenti informazioni:

lista dei servizi erogati (nome, descrizione, codifica, etc.);

infrastruttura tecnologica che ospita i servizi erogati con il dettaglio dei servizi tecnici che li compongono;

allarmi associati alle risorse infrastrutturali dei servizi tecnici che hanno impatto sui servizi erogati;

eventuali ticket di incidenti aperti dalla Società di cui all'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, per la gestione e la risoluzione degli allarmi.

b) vista di alto livello con rappresentazione, sia real time sia giornaliera, dell'andamento dello stato dei servizi erogati e dei relativi indicatori di disponibilità (eventi di infrastruttura, eventi da sonde end-to-end, ticket di incidenti);

c) rappresentazione dell'andamento della produzione dei servizi, in funzione dei livelli di autorizzazione definiti dal Ministero dell'interno, anche in termini di analisi delle interazioni del sistema con i soggetti che accedono (comuni, pubbliche amministrazioni, ed altri enti) e degli scostamenti dal trend, compresi report sintetici sullo stato di sicurezza del sistema.

#### 4. Protezione da attacchi informatici

Al fine di protezione dei sistemi operativi da attacchi informatici, eliminando le vulnerabilità, si utilizzano:

a) in fase di configurazione, procedure di hardening finalizzate a limitare l'operatività alle sole funzionalità necessarie per il corretto funzionamento dei servizi;

b) in fase di messa in esercizio, oltre che ad intervalli prefissati o in presenza di eventi significativi, processi di vulnerability assessment and mitigation nei software utilizzati e nelle applicazioni dei sistemi operativi;

c) piattaforma di sistemi firewall e sonde anti-intrusione.

Allegato D

### Servizi dell'ANPR

Il presente allegato descrive i servizi che ANPR assicura ai soggetti che accedono.

Le richieste di servizio sono elaborate in file XML o altri formati aperti.

La risposta del sistema può avere formato XML, ASCII o PDF o altri formati aperti.

I servizi sono erogati in modalità web service ovvero attraverso una web application fruibile dal sito internet della ANPR.

#### A) Servizi ai Comuni

##### A.1) Registrazione dei dati.

I servizi di registrazione consentono le operazioni di modificazione dei dati di competenza del comune, in tempo reale.

In risposta alla richiesta dell'operatore, in assenza di errore dell'operazione, il sistema invia la conferma di modificazione del dato ad un protocollo riferito all'operazione; in caso di errore, il comune riceve un avviso di esito negativo, con indicazione della causa.

Al comune è, inoltre, resa disponibile la consultazione delle operazioni richieste, del relativo esito, e dei relativi messaggi di conferma e di errore, per intervalli temporali, con le seguenti modalità:

l'esito di un'operazione di registrazione è disponibile per un anno;

gli eventi notificati al comune sono disponibili per centottanta giorni.

##### A. 2) Consultazione ed estrazione.

I servizi di consultazione consentono di interrogare l'ANPR per i dati di competenza, secondo i seguenti parametri:

per campi o combinazioni di campi;

per tipo di operazione;

per intervalli temporali.

In esito alla richiesta, il sistema comunica il numero

progressivo e la data della risposta; in presenza di errori nella richiesta, il sistema comunica l'esito negativo, con indicazione della causa.

I servizi di estrazione consentono al Comune di estrarre i dati di ANPR di propria competenza con modalita' analoghe a quelle descritte per i servizi di consultazione; in alternativa, il Comune puo' fornire ad ANPR una lista di soggetti per i quali ANPR restituira' in risposta i dati previsti per il tipo di estrazione prescelto dal Comune.

L'esito delle operazioni di consultazione ed estrazione e' disponibile per trenta giorni.

L'esito delle richieste di consultazione non esaudite in tempo reale e' disponibile per trenta giorni.

#### A. 3) Certificazione.

I servizi di emissione delle certificazioni anagrafiche di cui al capo VI del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, nonche' all'articolo 7 della legge 27 ottobre 1988, n. 470, sono erogati ai Comuni secondo le modalita' stabilite dal decreto legislativo 7 marzo 2005, n. 82.

Le richieste di certificazione sono esclusivamente di tipo puntuale e sono evase contestualmente.

In presenza di errore nella richiesta di emissione, il sistema comunica l'esito negativo, con indicazione della causa.

A. 4) Invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di cui all'articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396.

L'ANPR rende disponibile il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di cui all'articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, che pervengono ai comuni con le modalita' tecniche di cui al decreto del Ministro dell'interno previsto dall'articolo 2, comma 3, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

Con il medesimo servizio di invio del certificato di morte di cui al citato articolo 74, e' altresì inoltrata la denuncia della causa di morte di cui all'articolo 1 del decreto del Presidente della Repubblica 10 settembre 1990, n. 285.

#### A. 5) Servizi accessori.

I servizi accessori consentono di verificare lo stato delle operazioni richieste.

Comprendono, in particolare:

il servizio di notifica dell'esito delle operazioni e degli eventi di competenza per l'allineamento delle banche dati tenute dal Comune per lo svolgimento delle proprie funzioni e dei servizi non supportati dall'ANPR;

il servizio di verifica dell'esito di un'operazione;

il servizio di ricezione delle risposte rese disponibili da ANPR;

il servizio di annullamento dell'operazione;

il servizio di variazione di dati;

il servizio di consultazione delle notifiche;

il servizio di monitoraggio.

I dati che consentono ad ANPR di fornire i servizi in questione sono conservati per un periodo di tempo prefissato, trascorso il quale sono storicizzati nel modo seguente:

l'esito di un'operazione di registrazione e' disponibile per un anno;

l'esito delle operazioni di consultazione e' disponibile per trenta giorni;

gli eventi notificati al Comune sono disponibili per un periodo di centottanta giorni;

le risposte alle richieste di consultazione ed estrazione non esaudite in tempo reale rimangono disponibili per trenta giorni.

Sara' inoltre reso disponibile un servizio di interscambio in tempo reale delle comunicazioni di stato civile tra Comuni.



B) Servizi alle pubbliche amministrazioni e agli enti che erogano pubblici servizi

B.1) Consultazione ed estrazione

I servizi di consultazione ed estrazione consentono di interrogare i dati dell'ANPR di competenza, secondo specifici parametri di ricerca.

La pubblica amministrazione, utilizzando la propria applicazione, invia la richiesta di consultazione o estrazione e riceve in risposta il risultato della richiesta; qualora il numero di soggetti che verificano le condizioni richieste sia particolarmente elevato o il tipo di ricerca prescelto richieda elaborazioni complesse, ANPR attribuisce alla richiesta un numero progressivo e rende disponibile la risposta in un momento successivo. La Pubblica Amministrazione riceve in risposta il numero progressivo assegnato alla richiesta e la data in cui saranno resi disponibili gli esiti dell'elaborazione.

In presenza di errori nella struttura dei dati della richiesta, ANPR restituisce un esito negativo, motivando il motivo dello scarto.

B.2) Comunicazione dati e variazioni anagrafiche

L'ANPR rende disponibile alle pubbliche amministrazioni i dati e le variazioni anagrafiche di competenza registrate dai Comuni.

B.3) Servizi accessori

I servizi accessori consentono di verificare lo stato delle operazioni richieste e comprendono:

- il servizio di notifica dell'esito delle operazioni e degli eventi di competenza;

- il servizio di ricezione delle risposte dell'ANPR;

- il servizio di consultazione delle notifiche;

- il servizio di monitoraggio.

I dati che consentono ad ANPR di fornire i servizi in questione sono conservati per un periodo di tempo prefissato, trascorso il quale vengono storicizzati:

- l'esito delle operazioni di consultazione ed estrazione e' disponibile per trenta giorni;

- gli eventi notificati alla Pubblica Amministrazione sono disponibili per un periodo di centottanta giorni;

- le risposte alle richieste di consultazione ed estrazione non esaudite in tempo reale rimangono disponibili per trenta giorni.

## » DL 19/06/2015, n. 78

**DECRETO LEGGE 19 giugno 2015, n. 78** <sup>(1) (2) (4)</sup>.

**Disposizioni urgenti in materia di enti territoriali. Disposizioni per garantire la continuità dei dispositivi di sicurezza e di controllo del territorio. Razionalizzazione delle spese del Servizio sanitario nazionale nonché norme in materia di rifiuti e di emissioni industriali.** <sup>(3)</sup>

<sup>(1)</sup> Pubblicato nella Gazz. Uff. 19 giugno 2015, n. 140, S.O.

<sup>(2)</sup> Convertito in legge, con modificazioni, dall' *art. 1, comma 1, L. 6 agosto 2015, n. 125*.

<sup>(3)</sup> Titolo così modificato dalla *legge di conversione 6 agosto 2015, n. 125*. Precedentemente il titolo era il seguente: «Disposizioni urgenti in materia di enti territoriali.».

<sup>(4)</sup> In deroga a quanto disposto dal presente provvedimento vedi l' *art. 1, comma 717, L. 28 dicembre 2015, n. 208*.

---

### IL PRESIDENTE DELLA REPUBBLICA

Visti gli *articoli 77, 81 e 87 della Costituzione*;

Ritenuta la necessità e urgenza di definire gli obiettivi del patto di stabilità interno degli enti locali per l'anno 2015, come approvati con l'intesa sancita nella Conferenza Stato - Città ed autonomie locali del 19 febbraio 2015, in modo da consentire agli stessi di programmare la propria attività finanziaria e predisporre in tempi rapidi il bilancio di esercizio 2015;

Ritenuta la necessità e urgenza di attribuire spazi finanziari, anticipazioni di cassa e minori vincoli ai comuni anche al fine di consentire spese per specifiche finalità, in particolare per interventi di messa in sicurezza degli edifici scolastici e del territorio, compresi quelli derivanti da eventi calamitosi;

Ritenuta la necessità e urgenza di implementare le disposizioni finalizzate al collocamento dei dipendenti delle province, non essenziali all'espletamento delle funzioni ad esse residue;

Ritenuta la necessità e urgenza di consentire a città metropolitane, province e comuni la rinegoziazione dei mutui, la rimodulazione dei piani pluriennali di riequilibrio;

Ritenuta la necessità e urgenza di dettare disposizioni volte a incrementare ulteriormente la liquidità per il pagamento dei debiti certi, liquidi ed esigibili;

Ritenuta, altresì, la necessità e urgenza di specificare ed assicurare il contributo alla finanza pubblica da parte degli enti territoriali, come sancito nell'Intesa raggiunta in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nella riunione del 26 febbraio 2015;

Ritenuta la necessità e urgenza di dettare disposizioni finalizzate a migliorare ulteriormente gli obiettivi di trasparenza e di accelerazione nei processi di ricostruzione dopo il sisma del 6 aprile 2009; di prevedere l'istituzione di Zone Franche Urbane (ZFU) nell'ambito dei territori emiliani colpiti dal sisma del 20 e 29 maggio 2012 e dall'alluvione del 17 gennaio 2014 in favore delle microimprese; di dettare disposizioni finalizzate ad accelerare la ripresa sociale e imprenditoriale nell'ambito dei territori lombardi colpiti dall'alluvione del 20 e 29 maggio 2012; di prorogare il termine fissato dall'articolo 1, comma, 632 della legge n. 190 del 2014;

Ritenuta la necessità e l'urgenza di implementare l'Anagrafe nazionale della popolazione residente, includendovi i dati relativi allo stato civile e alle liste di leva, e di assicurare ai comuni la disponibilità di un sistema di controllo, gestione ed interscambio dei dati e servizi per lo svolgimento delle loro funzioni istituzionali, nonché di adottare misure per rafforzare i servizi per l'impiego ai fini dell'erogazione di

politiche attive del lavoro;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione dell'11 giugno 2015;

Sulla proposta del Presidente del Consiglio dei ministri, del Ministro dell'economia e delle finanze e del Ministro dell'interno;

EMANA

il seguente decreto-legge:

---

**Art. 10.** *Nuove disposizioni in materia di Anagrafe Nazionale della Popolazione Residente e di carta d'identità elettronica*

1. All'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, sono apportate le seguenti modifiche:

a) dopo il comma 2 è inserito il seguente: "2-bis. L'ANPR contiene altresì l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni e fornisce i dati ai fini della tenuta delle liste di cui all'articolo 1931 del codice dell'ordinamento militare di cui al decreto legislativo 15 marzo 2010, n. 66, secondo le modalità definite con uno dei decreti di cui al comma 6, in cui è stabilito anche un programma di integrazione da completarsi entro il 31 dicembre 2018.";

b) i primi due periodi del comma 3 sono sostituiti dai seguenti: "L'ANPR assicura ai singoli comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, e mette a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale. Al fine dello svolgimento delle proprie funzioni, ad eccezione di quelle assicurate dall'ANPR e solo fino al completamento dell'Anagrafe nazionale, il comune può utilizzare i dati anagrafici eventualmente conservati localmente, costantemente allineati con l'ANPR.".

2. Ai fini di cui al comma 1, il Ministero dell'interno, in attuazione dell'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, si avvale della società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. Le attività di implementazione dell'ANPR, ivi incluse quelle di progettazione, sono curate dal Ministero dell'interno d'intesa con l'Agenzia per l'Italia digitale.

3. All'articolo 7-vicies ter, del decreto-legge 31 gennaio 2005, n. 7, convertito, con modificazioni, dalla legge 31 marzo 2005, n. 43, il comma 2-bis è sostituito dal seguente: "2-bis. L'emissione della carta d'identità elettronica è riservata al Ministero dell'interno che vi provvede nel rispetto delle norme di sicurezza in materia di carte valori, di documenti di sicurezza della Repubblica e degli standard internazionali di sicurezza. Con decreto del Ministro dell'interno, di concerto con il Ministro per la semplificazione e la pubblica amministrazione ed il Ministro dell'economia e delle finanze, sentita l'Agenzia per l'Italia digitale, il Garante per la protezione dei dati personali e la Conferenza Stato-città autonomie locali, sono definite le caratteristiche tecniche, le modalità di produzione, di emissione, di rilascio della carta d'identità elettronica, nonché di tenuta del relativo archivio informatizzato." <sup>(5)</sup>

4. All'articolo 10 del decreto-legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, i commi 2 e 3 sono abrogati.

5. In attesa dell'attuazione del comma 3 si mantiene il rilascio della carta d'identità elettronica di cui all'articolo 7-vicies ter, comma 2, del decreto-legge 31 gennaio 2005, n. 7, convertito, con modificazioni, dalla legge 31 marzo 2005, n. 43.

6. Per gli oneri derivanti dai commi 1 e 3 del presente articolo è autorizzata la spesa per investimenti di 59,5 milioni di euro per l'anno 2015, di 8 milioni di euro l'anno 2016 e di 62,5 milioni di euro, ogni cinque anni, a decorrere dall'anno 2020 e, per le attività di gestione, di 2,7 milioni di euro a decorrere dall'anno 2016. Alla copertura dei relativi oneri si provvede, quanto a 59,5 milioni di euro per l'anno 2015, a 8 milioni di euro l'anno 2016 e a 62,5 milioni di euro, ogni cinque anni, a decorrere dall'anno 2020, mediante corrispondente utilizzo delle risorse, anche in conto residui, di cui all'articolo 10, comma 3-bis, del decreto-legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, e, quanto a 2,7 milioni di euro per l'anno 2016 e a 0,7 milioni di euro a decorrere dall'anno 2017, mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 10,

comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307, e quanto a 2 milioni di euro a decorrere dall'anno 2017, si provvede mediante corrispondente riduzione delle proiezioni dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2015-2017, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2015, allo scopo parzialmente utilizzando l'accantonamento relativo al medesimo Ministero. <sup>(6)</sup>

<sup>(5)</sup> Comma così modificato dalla *legge di conversione 6 agosto 2015, n. 125*.

<sup>(6)</sup> Vedi, anche, il *D.M. 23 dicembre 2015*.

---



**Agenzia per l'Italia Digitale**

*Presidenza del Consiglio dei Ministri*

## **REGOLAMENTO**

### **RECANTE LE MODALITÀ PER L'ACCREDITAMENTO E LA VIGILANZA DEI GESTORI DELL'IDENTITÀ 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 delle 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 2015, 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 15 settembre 2015.



## **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 a 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) il piano di test per le verifiche dell'Agenzia previste al par. 3 lettera b);
- n) documentazione delle prove di collaudo interno comprovanti l'aderenza dei protocolli di autenticazione adottati a tutti gli aspetti previsti dalle regole tecniche;



- o) documentazione delle prove di collaudo interno dei dispositivi usati per l'autenticazione informatica;
- 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 tracciate 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 e loro analisi al fine di sostenere la loro collocazione nel livello di sicurezza di cui al comma 1 dell'articolo 6 del DPCM 24 ottobre 2014 ritenuto appropriato. Al fine di distinguere nello scambio documentale con l'Agenzia le tipologie di credenziali fra loro, ad ogni tipologia è assegnato un riferimento univoco composto da *aaaa\_ss\_mm* dove, *aaaa* rappresenta l'anno in cui la tipologia di credenziali è presentata per la prima volta all'Agenzia per la valutazione prevista dal comma 2 del citato articolo del DPCM, *ss* è un numero sequenziale univoco nell'ambito di ogni singolo anno che individua la tipologia presentata nell'anno, *mm* è un numero sequenziale che afferisce alle eventuali modifiche successivamente presentate per la singola tipologia;
- 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.



## **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**

VISTO l'art. 4 del DPCM 24 ottobre 2014, che al comma 4 assegna all'Agenzia il compito di stabilire con proprio regolamento, le procedure necessarie a 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;

VISTO l'art. 7 del DPCM 24 ottobre 2014, che al comma 2, lettera e) prevede l'uso di soluzioni di identificazione informatica fornita da sistemi informatici preesistenti all'introduzione dello SPID che risultino aver adottato, a seguito di apposita istruttoria dell'Agenzia, regole di identificazione informatica caratterizzate da livelli di sicurezza uguali o superiori a quelli definiti nel DPCM medesimo;

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;

l'Agenzia per l'Italia Digitale emana il presente regolamento.

## **1. Obiettivi**

L'identità digitale, riconosciuta anche dalle pubbliche amministrazioni, è presente nel nostro Paese da diversi anni sotto varie forme, fornita da soggetti pubblici e privati per consentire l'accesso ai servizi in rete. Fino ad ora tali identità erano generalmente usabili per l'accesso ai servizi resi disponibili dal soggetto che le forniva. Con il sistema SPID c'è un cambio di paradigma: l'introduzione di un sistema federato di gestione dell'identità digitale consente ai titolari delle stesse di utilizzare le

medesime credenziali per l'accesso a servizi in rete eterogenei, resi disponibili da diversi fornitori di servizi in rete.

Tipici esempi sono le credenziali fornite da pubbliche amministrazioni, ma anche da soggetti privati, quali gli istituti bancari.

Al fine del riuso di identità digitali pregresse, il legislatore ha inserito all'articolo 7 del DPCM 24 ottobre 2014, la seguente disposizione:

*2. La verifica dell'identità del soggetto richiedente e la richiesta di adesione avvengono in uno dei seguenti modi:*

*e) identificazione informatica fornita da sistemi informatici preesistenti all'introduzione dello SPID che risultino aver adottato, a seguito di apposita istruttoria dell'Agenzia, regole di identificazione informatica caratterizzate da livelli di sicurezza uguali o superiori a quelli definiti nel presente decreto.*

Il presente regolamento, pubblicato sul sito istituzionale dell'Agenzia, descrive i requisiti generali che tali preesistenti sistemi devono possedere al fine di poter essere utilizzati al fine di ottemperare alla verifica dell'identità di un soggetto che richiede il rilascio di un'identità SPID e le modalità con cui l'Agenzia conduce l'istruttoria prevista.

## **2. Presentazione dell'istanza**

Al fine di utilizzare le soluzioni di identificazione informatica preesistenti di cui all'articolo 7, comma 2, lettera e) del DPCM 24 ottobre 2014, per la verifica dell'identità e la richiesta di adesione dei soggetti richiedenti un'identità SPID, il gestore dell'identità digitale può presentare apposita istanza all'Agenzia. L'istanza, 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, o da soggetto da questo delegato o incaricato, ed è inviata alla casella di posta elettronica certificata dell'Agenzia. Nell'istanza è indicato il nominativo del referente deputato alla sua gestione, un suo recapito telefonico e di posta elettronica.

## **3. Documentazione da inviare**

All'istanza è allegata la documentazione inerente il preesistente sistema di cui si chiede la valutazione, attestante:

1. Le modalità utilizzate nel processo di verifica dell'identità dei titolari delle identità pregresse;
2. Le modalità di raccolta e conservazione degli elementi comprovanti il processo di cui al





- precedente punto 1, atte a garantirne l'esibizione, l'integrità e l'autenticità;
3. Le modalità di individuazione della persona fisica che ha effettuato la verifica di cui al precedente punto 1;
  4. La specifica formazione del personale addetto alla verifica di cui al precedente punto 1;
  5. La modalità di consegna delle credenziali di autenticazione;
  6. Le modalità di raccolta e conservazione delle elementi comprovanti la consegna di cui al precedente punto 5, atte a garantirne l'esibizione, l'integrità e l'autenticità;
  7. La descrizione tecnica delle credenziali di autenticazione fornite;
  8. La descrizione tecnica di eventuali dispositivi hardware forniti per l'autenticazione;
  9. La descrizione tecnica di eventuali presidi software forniti per l'autenticazione;
  10. Eventuali attività aggiuntive che l'istante intende porre in essere al fine di fornire le nuove identità SPID;
  11. L'analisi dei rischi e delle contromisure afferenti l'uso delle identità pregresse ai fini della verifica dell'identità del soggetto richiedente l'identità SPID;
  12. Le modalità con cui ai soggetti titolari dell'identità pregressa è offerta la facoltà di utilizzare la stessa per ottenere un'identità SPID.
  13. Le informazioni fornite ai soggetti di cui al precedente punto 12 atte a chiarire l'assenza di qualunque obbligo a dotarsi di identità SPID, gli obblighi e le responsabilità assunte dal gestore dell'identità SPID, gli obblighi del titolare dell'identità digitale SPID, i rischi derivanti dal possesso della stessa, le cautele e le contromisure adottabili dal titolare.

#### **4. Iter istruttorio**

L'istruttoria relativa alle istanze di valutazione della conformità di sistemi di identificazione informatica preesistenti all'introduzione del sistema SPID, è effettuata dall'Agenzia che, al ricevimento dell'istanza, comunica al richiedente il nominativo e i riferimenti del responsabile del procedimento amministrativo al referente deputato alla gestione della stessa.

L'Agenzia si riserva di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato.

L'istanza di valutazione della conformità si considera accolta qualora non sia comunicato al richiedente il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

Il termine di novanta giorni di cui al periodo precedente, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione dell'istanza, esclusivamente per la motivata



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.

L'Agenzia si riserva la facoltà di svolgere verifiche presso le strutture utilizzate per il rilascio delle identità pregresse e di interloquire con addetti a tale attività al fine di verificarne la formazione. A tale scopo l'Agenzia presenta richiesta al gestore dell'identità digitale SPID attraverso il referente indicato nell'istanza presentata. Tale richiesta interrompe il termine di novanta giorni di cui sopra, che riprende a decorrere il giorno successivo il completamento delle verifiche.

Al termine dell'istruttoria, l'Agenzia accoglie l'istanza ovvero la respinge con provvedimento motivato e ne dà apposita comunicazione al richiedente. Nella medesima comunicazione l'Agenzia indica i livelli di sicurezza delle identità digitali di cui all'articolo 6 del DPCM 24 ottobre 2014 rilasciabili con le identità pregresse oggetto di valutazione.

Il gestore di identità SPID, ottenuto favorevole pronunciamento da parte dell'Agenzia, può iniziare ad utilizzare le credenziali fornite con le identità pregresse al fine di verificare l'identità dei richiedenti un'identità SPID e acquisirne la volontà.

Il soggetto la cui istanza sia stata respinta, non può presentare una nuova istanza per il medesimo oggetto se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente e, comunque, non prima che siano trascorsi di sei mesi dalla data di deposito dell'istanza respinta.

---



## **REGOLAMENTO**

### **RECANTE LE MODALITÀ ATTUATIVE PER LA REALIZZAZIONE DELLO SPID**

**(articolo 4, comma 2, DPCM 24 ottobre 2014)**

**Visto** il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale, e, in particolare, l'articolo 64 che prevede l'istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese” (di seguito: SPID);

**Visto** il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 che definisce le caratteristiche di SPID, nonché i tempi e le modalità di adozione dello stesso da parte delle pubbliche amministrazioni e delle imprese, e, in particolare, l'articolo 4, comma 2;

**Visto** il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

**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 e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta ufficiale dell'Unione europea serie L 257 del 28 agosto 2014;

**Sentito** il Garante per la protezione dei dati personali;

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

**CAPO I**  
**Disposizioni generali**

**Art. 1**  
**(Oggetto)**

1. Ai fini della realizzazione di SPID, il presente regolamento individua le modalità attuative:
- a) con cui i soggetti aderiscono al sistema, previo accreditamento e stipula di convenzioni;
  - b) di rilascio dell'identità digitale, previa verifica dell'identità del soggetto richiedente e rilascio delle credenziali;
  - c) di gestione del ciclo di vita dell'identità digitale, ivi compresa la sospensione e la revoca;
  - d) di autenticazione del soggetto che richiede il servizio;
  - e) di monitoraggio da parte dell'Agid.

**Art. 2**  
**(Il sistema pubblico per la gestione dell'identità digitale)**

SPID prevede diversi soggetti:

- a) l'utente, che potrà disporre di uno o più identità digitali, che contengono alcune informazioni identificative obbligatorie, come il codice fiscale, il nome, il cognome, il luogo di nascita, la data di nascita e il sesso;
- b) il gestore dell'identità digitale. Si tratta di un soggetto, che dovrà essere accreditato dall'Agenzia per l'Italia Digitale e che avrà il ruolo di creare e gestire le identità digitali;
- c) il gestore di attributi qualificati che, in base alle norme vigenti, può certificare attributi qualificati, come il possesso di un titolo di studio, l'appartenenza ad un ordine professionale;
- d) il fornitore di Servizi – soggetto pubblico o privato – che eroga servizi on-line, previo riconoscimento dell'utente da parte del gestore dell'identità digitale.

Il Sistema SPID si conforma al principio di necessità nel trattamento dei dati di cui all'articolo 3 del decreto legislativo 30 giugno 2003, n. 196, in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. I trattamenti dei dati personali in applicazione del presente regolamento sono effettuati esclusivamente per le finalità previste dall'articolo 64 del CAD e dall'articolo 2, comma 2, del DPCM 24 ottobre 2014 e con le modalità individuate dal presente regolamento, nel rispetto delle garanzie previste dal medesimo decreto legislativo n. 196 del 2003.

*Il sistema SPID è basato su tre livelli di sicurezza di autenticazione informatica.*

Il processo di autenticazione informatica è diretto alla verifica dell'identità digitale associata a un soggetto ai fini della erogazione di un servizio fornito in rete. A tale verifica di identità è associato un livello di sicurezza o di garanzia ( *level of assurance - LoA* ) progressivamente crescente in termini di sicurezza.



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

Il livello di sicurezza è il risultato dell'intero procedimento che sottende all'attività di autenticazione. Tale processo va dalla preliminare associazione tra un soggetto e un'identità digitale che lo rappresenta in rete, con annessa attribuzione di credenziali in grado di comprovare tale associazione, ai meccanismi che realizzano il protocollo di autenticazione al momento della richiesta di un servizio in rete.

In SPID sono definiti tre livelli di sicurezza, corrispondenti ad altrettanti livelli specificati nella ISO-IEC 29115. In particolare:

- a) livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115): garantisce con un buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato applicabile nei casi in cui il danno causato, da un utilizzo indebito dell'identità digitale, ha un basso impatto per le attività del cittadino/impresa/amministrazione;
- b) livello 2 (corrispondente al LoA3 dell'ISO-IEC 29115): garantisce con un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio ragguardevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno consistente;
- c) livello 3 (corrispondente al LoA4 dell'ISO-IEC 29115): garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato 3 della Direttiva 1999/93/CE; questo è il livello di garanzia più elevato e da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno serio e grave.

Ai sensi dell'articolo 6, commi 4 e 5, del DPCM 24 ottobre 2014 (di seguito: "DPCM"), i fornitori di servizi scelgono il livello di sicurezza SPID necessario per accedere ai propri servizi e non possono discriminare l'accesso ai propri servizi sulla base del gestore di identità che l'ha fornita.

Nell'Appendice A è riportata, a titolo esemplificativo, una metodologia da adottare allo scopo.

### *Art. 3*

*(Adesione a SPID)*

*Possono aderire a SPID:*

- a) i gestori dell'identità digitale e i gestori di attributi qualificati, previo accreditamento e stipula di apposite convenzioni con Agid secondo le modalità definite con regolamento adottato ai sensi dell'articolo 4, comma 3, del DPCM 24 ottobre 2014; i gestori dell'identità digitale sono tenuti inoltre ad aderire alle apposite convenzioni che l'Agenzia stipula con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità;



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

- b) i fornitori dei servizi stipulando una convenzione con l’Agenzia. Ai fini della stipula, i fornitori dei servizi indicano all’Agenzia i servizi erogati e, per ciascuno di questi servizi, motivano le scelte in relazione ai livelli di sicurezza adottati e alla necessità di informazioni richieste relative ad attributi identificativi, non identificativi e qualificati. Per i servizi qualificati, i predetti soggetti motivano le circostanze per cui le informazioni sono necessarie e non eccedenti per l’erogazione dei singoli servizi.

Aderiscono a SPID le pubbliche amministrazioni di cui all’articolo 2, comma 2, del CAD, entro i ventiquattro mesi successivi all’accreditamento del primo gestore dell’identità digitale.

L’Agenzia vigila sull’operato dei soggetti che partecipano a SPID.

#### *Art. 4*

##### *(Rilascio e gestione delle identità digitali SPID)*

Il rilascio dell’identità digitale SPID e la gestione del ciclo di vita della stessa da parte dei gestori dell’identità digitale sono così articolati:

1) Il rilascio delle identità digitali si articola nei seguenti processi:

- a) richiesta dell’identità digitale e identificazione del richiedente;
- b) esame e verifica dell’identità del richiedente;
- c) conservazione e registrazione dei documenti;
- d) emissione dell’identità digitale;
- e) creazione e consegna delle credenziali.

2) La gestione del ciclo di vita dell’identità digitale si articola nei seguenti processi:

- a) gestione degli attributi;
- b) sospensione e revoca dell’identità;
- c) gestione del ciclo di vita delle credenziali che si articola in:
  - 1) conservazione;
  - 2) sospensione e revoca;
  - 3) rinnovo e sostituzione.

#### *CAPO II*

##### *Rilascio delle identità digitali*

#### *Art. 5*

##### *(Richiesta dell’identità digitale)*

Le identità digitali sono rilasciate dal gestore dell’identità digitale, su richiesta di un soggetto interessato secondo quanto previsto dall’art. 7 del DPCM mediante presentazione di un modulo di *richiesta di adesione* che contiene tutte le informazioni necessarie per l’identificazione del soggetto richiedente.

Il modulo di *richiesta di adesione* contiene:



- a) i dati identificativi del richiedente, che costituiscono gli attributi identificativi dell'identità digitale;
- b) le informazioni che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali e il richiedente dell'identità digitale, che costituiscono gli attributi secondari dell'identità digitale;

Per le persone fisiche sono obbligatorie le seguenti informazioni:

- a) cognome e nome;
- b) sesso, data e luogo di nascita;
- c) codice fiscale;
- d) estremi di un valido documento di identità
- e) gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM .

Per le persone giuridiche sono obbligatorie le seguenti informazioni:

- a) denominazione/ragione sociale;
- b) codice fiscale o P.IVA (se uguale al codice fiscale);
- c) sede legale;
- d) visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale);
- e) estremi del documento di identità utilizzato dal rappresentante legale;
- f) gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM .

Per gli attributi secondari, sono forniti almeno un indirizzo di posta elettronica e un recapito di telefonia mobile, entrambi verificati dal gestore di identità digitale nel corso del processo di identificazione, inviando un messaggio di posta all'indirizzo dichiarato, contenente una URL per la verifica e un SMS al numero di cellulare con un codice numerico di controllo che deve essere riportato in risposta. Inoltre, per quanto riguarda l'indirizzo di posta elettronica, i gestori dovranno accertarsi, oltre che lo stesso sia un indirizzo corrispondente a una reale casella di posta, che sia unico in ambito SPID, ovvero che esso non sia stato precedentemente indicato dallo stesso soggetto per l'acquisizione di una identità digitale SPID presso lo stesso o un altro gestore dell'identità digitale. Tale controllo potrà essere effettuato anche consultando la directory delle identità SPID. Nel caso tale verifica non dovesse andare a buon fine il gestore dovrà dare obbligo al richiedente dell'indicazione di un indirizzo alternativo. Nel caso il richiedente non disponesse di tale indirizzo alternativo, il gestore dell'identità digitale, d'accordo con il richiedente, dovrà provvedere esso stesso al rilascio di una casella di posta avente un idoneo indirizzo. In questo caso il gestore delle identità digitali deve garantire l'inoltro automatico di tutte le mail ricevute su



questo nuovo indirizzo all'indirizzo di posta elettronica originariamente dichiarato dal soggetto richiedente.

Nel modulo, il soggetto richiedente sottoscrive l'apposita dichiarazione con cui si assume la responsabilità, ai sensi dell'articolo 76 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, della veridicità delle informazioni fornite.

#### *Art. 6*

##### *(Identificazione del soggetto richiedente)*

Al ricevimento della richiesta, il gestore dell'identità digitale procede all'identificazione del soggetto richiedente, che consiste nell'accertamento delle informazioni sufficienti a identificare il soggetto richiedente sulla base di documenti forniti dallo stesso. Tale processo è effettuato da personale qualificato e opportunamente formato.

Le modalità di consegna della richiesta e il supporto utilizzato (cartaceo o digitale) dipendono da quale modalità, tra quelle previste dall'art. 7 del DPCM il gestore dell'identità digitale adotta per operare il processo di identificazione.

Il gestore dell'identità digitale, per una corretta e sicura attuazione del processo,

- a) fornisce l'informativa sul trattamento dei dati (articolo 13 del D.lgs. 196 del 2003);
- b) si assicura che il richiedente sia consapevole dei termini e delle condizioni associati all'utilizzo del servizio di identità digitale;
- c) si assicura che il richiedente sia consapevole delle raccomandazioni e delle precauzioni da adottare per l'uso delle identità digitali;
- d) acquisisce i dati necessari alla dimostrazione di identità.

#### *Art. 7*

##### *(Identificazione a vista del soggetto richiedente)*

Nel caso di identificazione a vista del soggetto richiedente presso le sedi allo scopo individuate si procede con l'acquisizione del modulo di *richiesta di adesione* in formato cartaceo compilato e sottoscritto dall'utente e con l'esibizione di un valido documento di identità.

Nel caso in cui il soggetto richiedente sia una persona giuridica, deve essere fornita la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che sottoscrive e presenta l'istanza. Il rappresentante legale dovrà a sua volta essere identificato tramite un valido documento d'identità.

L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento integro e in corso di validità rilasciato da un'Amministrazione dello Stato,





munito di fotografia e firma autografa dello stesso e controlla la validità del codice fiscale verificando la tessera sanitaria anch'essa in corso di validità.

Se i documenti esibiti dal richiedente risultano carenti delle caratteristiche di cui sopra, deve esserne esclusa l'ammissibilità e il processo di iscrizione deve essere sospeso o bloccato fino all'esibizione di documenti validi e integri.

**Art. 8**  
***(Identificazione a vista da remoto )***

L'identificazione a vista della persona fisica richiedente un'identità SPID da parte del gestore dell'identità può essere effettuata dai gestori dell'identità digitale anche in digitale da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196.

L'identificazione da remoto deve avvenire in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte dell'utente nel rispetto delle seguenti condizioni:

- a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;
- b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi.
- c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

Il gestore è responsabile della valutazione in merito alla sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del soggetto.

L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso, rilasciato da un'Amministrazione dello Stato e verifica il codice fiscale tramite la tessera sanitaria in corso di validità.

L'operatore che effettua l'identificazione può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente (ad esempio perché logoro o carente delle caratteristiche elencate).

La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale con modalità crittografiche atte a garantirne l'accesso esclusivamente



dietro richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, dell'utente e dell'autorità giudiziaria in caso di disconoscimento della stessa.

Nel caso l'identificazione a vista da remoto sia solo una delle modalità predisposte per la verifica dell'identità del richiedente, il gestore dell'identità deve richiedere il consenso al trattamento dei dati personali contenuti nelle riprese audio-video, specificando tale aspetto nell'informativa da rendere all'interessato ai sensi dell'articolo 13 del Codice.

La sessione audio/video deve essere condotta seguendo una procedura scritta e formalizzata dal gestore che prevede almeno le seguenti attività:

- a) l'acquisizione del consenso alla videoregistrazione e alla sua conservazione per 20 anni come previsto dalla normativa vigente in materia. L'operatore informa che la videoregistrazione sarà conservata in modalità protetta;
- b) l'operatore dichiara i propri dati identificativi;
- c) il soggetto conferma le proprie generalità;
- d) il soggetto conferma la data e l'ora della registrazione;
- e) il soggetto conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;
- f) il soggetto conferma il proprio numero di telefonia mobile e l'indirizzo mail;
- g) l'operatore invia un sms che il soggetto richiedente è tenuto a esporre al dispositivo di ripresa e una mail all'indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;
- h) l'operatore chiede e ottiene conferma dal soggetto circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;
- i) l'operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);
- j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;
- k) il soggetto conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;
- l) l'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;



- m) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati in base all'articolo 7, commi 8 e 9 del DPCM.

#### **Art. 9**

##### ***(Identificazione informatica tramite documenti digitali di identità)***

Nel caso di identificazione informatica tramite documenti digitali di identità, si procede con l'acquisizione del modulo di *richiesta di adesione* in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto elettronicamente (ad esempio con firme qualificate valide solo per la sessione in corso o per un periodo limitato). L'identificazione avviene tramite verifica dei documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi. Questa modalità di identificazione si basa su una presunzione di correttezza relativa al processo di identificazione espletato dal gestore che ha precedentemente rilasciato un documento digitale di identità.

#### **Art. 10**

##### ***(Identificazione informatica tramite altre identità SPID)***

Nel caso di identificazione informatica tramite altre identità SPID si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto elettronicamente (ad esempio con firme qualificate valide solo per la sessione in corso o per un periodo limitato). L'identificazione avviene attraverso l'accesso, utilizzando credenziali SPID di livello di sicurezza pari o superiore a quella oggetto della richiesta, a un servizio reso disponibile allo scopo da parte del gestore dell'identità digitale. Questa modalità di identificazione è applicabile quando la richiesta di una nuova identità è effettuata presso lo stesso gestore che ha rilasciato l'identità SPID utilizzata per la richiesta.

#### **Art. 11**

##### ***(Identificazione informatica tramite firma elettronica qualificata o firma digitale)***

Nel caso di identificazione informatica tramite firma elettronica qualificata o firma digitale si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto con firma elettronica qualificata o con firma digitale. L'identificazione avviene tramite la verifica della firma elettronica qualificata o firma digitale apposta sulla richiesta. Anche in questo caso il gestore delle identità digitali, considera che la fase di identificazione sia stata correttamente espletata dal fornitore di firma elettronica qualificata o digitale.



**Art. 12**  
**(Verifica dell'identità dichiarata)**

La verifica dell'identità consiste nel rafforzamento del livello di attendibilità degli attributi di identità, raccolti in fase di identificazione, compiuta attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti.

L'accesso alle fonti autoritative da parte dei gestori dell'identità ai fini dell'attività di verifica è effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445.

I gestori dell'identità digitale e i gestori degli attributi qualificati, usufruiscono del servizio di verifica del codice fiscale e dei dati anagrafici ad esso strettamente correlati fornito dall'Agenzia delle Entrate.

Sia il processo di identificazione che il processo di verifica sono eseguiti allo scopo di ottenere un adeguato grado di affidabilità, tenuto conto anche dello specifico livello di sicurezza di SPID.

Le tabelle seguenti rappresentano i requisiti relativi alle verifica di identità in relazione al livello di sicurezza nel caso di persona fisica e di persona giuridica.

Livello di sicurezza	Requisiti
Per tutti i livelli SPID	<p>1) Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata.</p> <p>2) I documenti sono autentici e validi sulla base di quanto risulta da soggetti istituzionali competenti (articolo 4, comma 1, lettera c del DPCM o, in assenza di convenzioni con l'Agenzia, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445). Il richiedente viene identificato usando le informazioni ottenute da soggetti istituzionali competenti con i quali l'Agenzia stipulerà apposite convenzioni..</p>

**Requisiti da soddisfare/Livelli di sicurezza SPID (persona fisica)**



Livello di garanzia	Requisiti
Per tutti i livelli SPID	<p>1) L'esistenza della persona giuridica è basata su evidenze riconosciute dal sistema delle imprese in ambito nazionale.</p> <p>2) Le evidenze sono tutte valide e autentici sulla base di quanto risulta da soggetti istituzionali competenti.</p> <p>3) Effettuata l'associazione amministratore o rappresentante legale, all'impresa-persona giuridica, si procede alla verifica - come persona fisica - dell'amministratore o del legale rappresentante, come indicato nella tabella precedente per l'identificazione di una persona fisica.</p>

#### Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)

In merito alle possibili minacce associabili al processo di verifica dell'identità, si veda l'Appendice B al presente documento.

#### Art. 13

##### *(Conservazione e registrazione dei documenti)*

Il processo di registrazione dei documenti completa la fase di rilascio di un'identità SPID a un soggetto. La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione.

I gestori dell'identità digitale, al fine di poter documentare la corretta esecuzione dei precedenti processi relativi all'attività di rilascio e di una identità, conservano i riscontri relativi ai processi di identificazione e verifica.

In merito al processo di richiesta e identificazione del richiedente devono essere conservati:

- 1) nel caso di identificazione tramite esibizione a vista:
  - a) identificazione "de visu": copia per immagine di tutta la documentazione esibita (documento d'identità e codice fiscale per persone fisiche, procura per persone giuridiche) e modulo di richiesta su supporto cartaceo sottoscritto in modalità autografa;
  - b) identificazione remota con strumenti audio/video: i dati di registrazione, nonché l'esplicita volontà del soggetto di dotarsi di identità digitale memorizzati in file audio-video, immagini e metadati strutturati in formato elettronico ;
- 2) nel caso di identificazione informatica:
  - a) log della transazione;



- b) modulo di *richiesta di adesione* in formato digitale sottoscritto elettronicamente o digitalmente (es. con firme qualificate valide solo per la sessione in corso o per un periodo limitato);
- 3) nel caso di firma elettronica qualificata o digitale:
  - a) modulo di *richiesta di adesione* allo SPID in formato digitale sottoscritto digitalmente;
  - b) tutti i documenti e dati utilizzati per l'associazione e la verifica degli attributi.

In merito al processo di verifica devono essere conservati i riscontri ottenuti a seguito degli accessi alle fonti autoritative.

Tutta la documentazione inerente alla creazione e al rilascio di una identità digitale deve essere conservata ai sensi dell'articolo 7, commi 8 e 9, del DPCM.

#### Art. 14 (Emissione dell'identità digitale)

Espletate con successo tutte le attività previste dai processi precedenti, l'identità digitale viene creata e rilasciata dal gestore. L'identità digitale è costituita da un insieme di attributi:

- a) attributi identificativi, come specificato dalla lettera c) del comma 1 dell'articolo 1 del DPCM;
- b) attributi secondari, come specificato dalla lettera d) del comma 1 dell'articolo 1 del DPCM ;
- c) codice identificativo, come specificato dalla lettera d) del comma 1 dell'articolo 1 del DPCM ;
- d) identificativo Utente;

Il *codice identificativo* è assegnato dal gestore dell'identità digitale, deve essere univoco in ambito SPID. Tale *codice identificativo* è definito dalla seguente regola:

*<codice Identificativo> = <cod\_IdP><numero unico>*

Dove:

- a) *<cod\_IdP>*: è un codice composto da 4 lettere;
- b) *<numero unico>*: è un codice alfanumerico composto da 10 caratteri univoco nel dominio del gestore.

#### Sezione IV Rilascio e consegna delle credenziali SPID

#### Art. 15 (Creazione delle credenziali)

1. Il processo di creazione delle credenziali comprende le attività necessarie a dare origine ad una credenziale o ai mezzi per la sua produzione.



2. In alcuni casi le credenziali, o i mezzi usati per la loro produzione, richiedono una fase di pre-elaborazione prima della loro emissione, ad esempio personalizzazioni sulla base dell'identità a cui esse vengono rilasciate. In questi casi la personalizzazione può avvenire secondo diverse modalità in relazione alla tipologia di credenziale da emettere (ad esempio la personalizzazione di un dispositivo (card, token) che contiene le credenziali può includere la stampa (all'esterno del dispositivo) o la scrittura (sul chip del dispositivo) del nome del soggetto per cui le credenziali saranno emesse). Ovviamente alcune tipologie di credenziali, ad esempio la password, non richiedono alcun intervento di personalizzazione.

Segue l'attività di inizializzazione delle credenziali operata al fine di assicurare che tutti i mezzi usati per la loro produzione siano successivamente idonei a supportare tutte le funzionalità attese. Per esempio, potrebbe essere richiesto che il chip della smart card calcoli la coppia di chiavi crittografiche. Analogamente, una smart card potrebbe essere emessa in uno stato "bloccato" e richiedere un PIN nel successivo processo di attivazione. Deve essere pure definita un'associazione fra una credenziale, o i mezzi usati per la sua produzione, e il soggetto per la quale viene emessa.

Le modalità con cui viene operata tale associazione e il legame instaurato tra le credenziali e l'utente a cui afferiscono, dipendono anche dal livello di sicurezza SPID per il quale le stesse credenziali sono rilasciate.

### ***livello 1 SPID***

Per il livello 1 SPID (corrispondente al LoA2 dell'ISO-IEC 29115) sono accettabili credenziali composte da un singolo fattore (ad es. password).

In particolare, in relazione al tipo della password, si raccomanda di adottare regole per ottenere password complesse e difficilmente attaccabili rispettando almeno i seguenti accorgimenti:

- a) lunghezza minima di otto caratteri;
- b) uso di caratteri maiuscoli e minuscoli;
- c) inclusione di uno o più caratteri numerici;
- d) non deve contenere più di due caratteri identici consecutivi.
- e) inclusione di almeno un carattere speciali ad es #, \$,% ecc.

Si raccomanda poi di vietare l'uso di formati comuni (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).

Le password devono avere una durata massima non superiore a 180 giorni e non possono essere riusate, o avere elementi di similitudine, prima di cinque variazioni e comunque non prima di 15 mesi: in questa materia resta valida la normativa prevista dal Codice in materia di protezione dei dati personali (Artt. da 33 a 36) e, in particolare, dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Codice privacy) aggiornato periodicamente in relazione all'evoluzione tecnica e all'esperienza maturata nel settore. Il Gestore dell'Identità adotta una procedura di sollecito con la quale invita l'utente a modificare la Password. )



### ***livello 2 SPID***

Per il livello 2 SPID (corrispondente al LoA3 dell'ISO-IEC 29115), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori, non necessariamente basati su certificati digitali.

In questo caso è accettabile l'utilizzo di una password (come sopra descritto) e l'adozione di una OTP generata con l'ausilio di un dispositivo fisico, l'invio di un SMS, liste-tabelle predefinite o applicazioni mobile per smartphone *o tablet collegati in rete* ; resta chiaro che, trattandosi di un OTP, la sua validità è limitata solo ad una transazione nell'ambito della sessione applicativa e per un tempo limitato e dipendente dal contesto del servizio richiesto.

### ***livello 3 SPID***

Per il livello 3 SPID (corrispondente al LoA4 dell'ISO-IEC 29115), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori, basati su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell' Allegato 3 della Direttiva 1999/93/CE.

In merito alle possibili minacce che possono essere associabili alle varie tipologie di token, si veda l'Appendice B al presente documento. In appendice D è inoltre riportata una tassonomia dei tipi di token.

## **Art. 16** ***(Consegna delle credenziali)***

Anche in questo caso, la complessità del processo dipende dal livello di sicurezza di autenticazione informatica SPID associato alla determinata credenziale. La consegna delle credenziali deve essere operata con modalità e strumenti che assicurino che la stessa sia effettuata al legittimo destinatario con adeguati criteri di riservatezza che salvaguardino il contenuto.

Per alti livelli di sicurezza deve essere prevista una consegna con attestazione dell'effettivo ricevimento delle credenziali; per dispositivi software ciò può essere fatto attraverso sessioni protette per la spedizione in modalità elettronica che assicurino la verifica della corrispondenza tra richiedente dell'identità e destinatario delle credenziali. Per livelli più bassi può essere sufficiente inviare una password o un PIN direttamente all'indirizzo fisico, ad esempio con posta raccomandata, al domicilio elettronico, tramite posta elettronica o PEC, oppure tramite comunicazioni inviate al dispositivo mobile del titolare (smartphone, tablet, cellulare, ecc.)

Il gestore delle identità digitali nella consegna delle credenziali garantisce:

- a) che il richiedente sia espressamente informato in modo compiuto e chiaro riguardo:
  - 1) agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali;





- 2) sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;
- b) la rispondenza del proprio sistema di sicurezza dei dati alle misure di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196.

**Art. 17**  
*(Attivazione delle credenziali)*

L'attivazione delle credenziali è il processo durante il quale le credenziali o i mezzi usati per produrle, sono rese effettivamente operative e pronte all'utilizzo.

Il processo di attivazione dipende direttamente dalla tipologia di credenziali adottate, ad esempio in alcuni casi le credenziali sono definite in uno stato di blocco quando sono inizializzate e restano in questo stato fino alla consegna al soggetto richiedente, in modo da prevenire qualsiasi abuso. In altri casi può essere prevista una password o codice iniziale per lo sblocco delle credenziali. Si consideri pure che le credenziali possono essere attivate anche successivamente ad una sospensione, quando ad esempio la loro validità sia stata temporaneamente annullata.

**Art. 18**  
*(Segnalazioni sull'utilizzo delle credenziali)*

Il gestore dell'identità digitale, su richiesta dell'utente, segnala via email o via sms, rispettivamente alla casella di posta o sul riferimento telefonico indicato dall'utente ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari a tale scopo indicato dall'utente.

**CAPO III**  
*Gestione del ciclo di vita dell'identità digitale*

**Art. 19**  
*(Gestione attributi)*

L'utente è tenuto a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del gestore, i contenuti degli attributi identificativi di seguito elencati.

- a) Per le persone fisiche:
  - 1. estremi del documento di riconoscimento e relativa scadenza;
  - 2. gli attributi secondari così come definiti all'articolo 1, comma d) del DPCM;
- b) Per le persone giuridiche:
  - 1. indirizzo sede legale



2. codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
3. rappresentante legale della società
4. attributi secondari così come definiti all'articolo 1, comma d) del DPCM

L'utente, in caso di dichiarazioni non fedeli o mendaci, si assume le responsabilità previste dalla legislazione vigente:

Le modalità operative per gli aggiornamenti devono essere rese possibili attraverso un'area web dedicata del gestore delle identità digitali accessibile mediante le credenziali SPID, almeno di livello due, in possesso dell'utente.

4. Il gestore dell'identità digitale deve inoltre prevedere un servizio di help desk tramite mail o compilando un form on-line sul sito web. Inoltre potrà essere previsto un sistema attraverso il quale l'utente potrà effettuare autonomamente alcune operazioni.

Ad ogni variazione da operare sugli attributi relativi ad una identità, il gestore dell'identità digitale, prima di aggiornare i dati registrati, deve eseguire le fasi di esame e verifica in relazione al livello SPID associato all'identità digitale. La richiesta di aggiornamento e aggiornamento devono essere notificati all'utente utilizzando un attributo secondario funzionale alle comunicazioni (ad es. l'indirizzo di posta elettronica se non è stato modificato durante la sessione di aggiornamento).

Futuri sviluppi potranno includere aggiornamenti automatici sulla base di modifiche degli attributi identificativi o secondari effettuati da pubbliche amministrazioni (ad es. ANPR, comuni, motorizzazione ecc.).

#### Art. 20

##### *(Sospensione e revoca dell'identità digitale)*

Ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il gestore revoca l'identità digitale nei casi seguenti:

- 1) risulta non attiva per un periodo superiore a 24 mesi;
- 2) per decesso della persona fisica;
- 3) per estinzione della persona giuridica;
- 4) per uso illecito dell'identità digitale;
- 5) per richiesta dell'utente;
- 6) per scadenza contrattuale.

Nel caso previsto dai punti 1 e 6, il gestore dell'identità digitale revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca al utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).



Nei casi previsti dai punti 2 e 3, il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

Nel caso previsto dal punto 4, ovvero nel caso in cui il utente ritenga che la propria identità digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione con una delle seguenti modalità:

- a) richiesta al gestore inviata via PEC;
- b) richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica, inviata tramite la casella di posta appositamente predisposta dal gestore.

Il gestore deve fornire esplicita evidenza al utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.

Contestualmente il utente potrà richiedere al fornitore dei servizi presso il quale ritiene che la propria identità sia stata utilizzata fraudolentemente il blocco all'accesso della propria identità inviando una richiesta in tal senso con le stesse modalità sopra previste ad una casella di posta appositamente predisposta dal fornitore di servizi.

Trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione. In caso contrario l'identità digitale viene ripristinata.

Nel caso previsto dal punto 5, l'utente può chiedere al gestore dell'identità digitale, , in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità analoghe a quelle previste dal precedente punto 4, ovvero attraverso:

- c) richiesta al gestore inviata via PEC;
- d) richiesta inviata tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale o elettronica;

Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.

La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.

I gestori dell'identità digitale conservano la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale

## Art. 21

### *(Gestione del ciclo di vita delle credenziali)*

*La gestione del ciclo di vita delle credenziali può comprendere i seguenti processi:*

- a) creazione delle credenziali;



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

- b) consegna delle credenziali o dei mezzi usati per la loro produzione;
- c) attivazione delle credenziali o dei mezzi usati per la loro produzione;
- d) conservazione delle credenziali;
- e) sospensione e revoca delle credenziali o mezzi usati per la loro produzione;
- f) rinnovo e sostituzione delle credenziali o mezzi usati per la loro produzione;

Alcuni dei processi sopra elencati possono essere influenzati dal fatto che le credenziali siano rese operative attraverso l'ausilio di un dispositivo hardware.

In merito alle possibili minacce associate al processo di emissione delle credenziali, si veda l'Appendice B al presente documento.

Adeguate documentazione deve essere conservata per tutto il ciclo di vita di una credenziale. Come condizione minima, la documentazione dovrà essere mantenuta per avere traccia delle seguenti informazioni:

- a) la creazione della credenziale
- b) l'identificativo della credenziale;
- c) il soggetto per il quale è stata emessa;
- d) lo stato della credenziale.

Opportuna documentazione sarà conservata per ogni sottoprocesso (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) del processo di gestione delle credenziali, nel pieno rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Dovranno essere conservate almeno le informazioni relative alla data di creazione della credenziale, allo stato della stessa, alle date di consegna, di attivazione (se prevista) e di eventuale sospensione, revoca o cancellazione.

#### *Art. 22 (Conservazione delle credenziali)*

Questo processo riguarda la conservazione delle credenziali o dei mezzi usati per loro produzione, in modo da garantirne la protezione contro abusi ed usi non autorizzati.

A livello 1 SPID, i file delle credenziali devono essere protetti da un sistema di controllo in modo da limitare l'accesso agli amministratori e alle applicazioni autorizzate.

Questi file non devono mai contenere le password in chiaro; allo scopo possono essere usate tecniche, come da standard internazionali e approvate dall'Agenzia, di crittografia o algoritmi di salt e hashing. A livello 2 e 3 SPID, vale quanto indicato a livello 1 con i necessari allineamenti e conformità agli standard e alla normativa vigente per i moduli crittografici e di sicurezza software/hardware.



**Art. 23**  
***(Sospensione e revoca delle credenziali)***

La revoca è il processo che annulla definitivamente la validità delle credenziali. Diversamente, la sospensione è associata ad un processo di annullamento temporaneo.

La revoca è disposta nei seguenti casi:

- 1) smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria);
- 2) utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto;
- 3) emissione di una nuova credenziale in sostituzione di una già in possesso dell'utente; emissione di una nuova credenziale in sostituzione di una scaduta.

Nel caso previsto dal numero 1, l'utente deve effettuare immediata richiesta di sospensione delle credenziali. Se la richiesta dell'utente non viene effettuata tramite posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identità digitale deve verificare, anche attraverso uno o più attributi secondari, la provenienza della richiesta di sospensione da parte del soggetto utente.

Il gestore dell'identità digitale sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Durante questo periodo può accadere che:

- a) il richiedente annulla la richiesta di sospensione (ad es. per ritrovamento) e quindi l'identità digitale viene ripristinata;
- b) il richiedente formalizza la richiesta presentando copia della denuncia presentata all'autorità giudiziaria, quindi l'identità digitale viene revocata.

In assenza di quanto indicato nelle lettere a) o b), l'identità digitale sarà automaticamente ripristinata scaduto il periodo di 30 giorni dalla data della richiesta.

Nel caso previsto dal numero 2, anche a seguito di segnalazioni ai sensi dell' articolo 8, comma 4 del DPCM, l'utente richiede la sospensione immediata dell'identità digitale al gestore del servizio. Si veda il paragrafo sulla sospensione e revoca dell'identità digitale.

**Art. 24**  
***(Rinnovo e sostituzione delle credenziali)***

Alcune tipologie di credenziali prevedono una scadenza temporale per l'uso. In questo caso il gestore dovrà provvedere tempestivamente alla creazione di una nuova credenziale da consegnare all'utente in sostituzione della vecchia scaduta. Situazione analoga è quella della sostituzione di una credenziale a seguito di guasto o per upgrade tecnologico ( ad esempio nel caso di credenziali di livello 3 passaggio da



chiavi da 128 bit a quelle da 256). Il gestore dell'identità, nel primo caso su richiesta dell'utente, nel secondo su sua iniziativa, emette la nuova credenziale e revoca automaticamente la vecchia.

In entrambi i casi devono essere previsti meccanismi con i quali il gestore comunica la revoca all'utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Si noti che, per alcune tipologie di credenziali, come ad es. quelle contenute su un dispositivo, può essere prevista (successivamente alla sua revoca) anche la distruzione fisica.

## CAPO IV Utilizzo di SPID

### Art. 25 (Autenticazione)

L'autenticazione è il processo in cui l'utente, usando le proprie credenziali SPID, dimostra la propria identità al gestore dell'identità digitale al fine di accedere a servizi disponibili in rete. Per la realizzazione del processo di autenticazione, SPID adotta il modello federato delle identità digitali definito dalle specifiche SAML emesse dal consorzio OASIS ( cfr *Regole Tecniche SPID*).

Le relazioni tra i soggetti coinvolti nel processo (*l'utente, il gestore dell'identità digitale, il fornitore di servizi* ed, eventualmente, *il gestore di attributi qualificati*) si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata dal soggetto titolare di una identità digitale, portano all'autorizzazione o al diniego della fruizione di un servizio erogato da un fornitore di servizi. Tali interazioni determinano la produzione di certificazioni (Asserzioni nella nomenclatura SAML) da parte dei *gestori delle Identità digitali* ed, eventualmente, dei *gestori di attributi qualificati*, e l'utilizzo delle stesse da parte dei *fornitori di servizi*.

I passaggi previsti sono i seguenti:

- 1) il *titolare dell'identità digitale* richiede l'accesso ad un servizio collegandosi telematicamente al portale del *fornitore di servizi*;

Il *fornitore dei servizi*, per poter procedere, deve individuare il *gestore dell'Identità digitale* in grado di autenticare il soggetto richiedente. Per far ciò il *gestore dell'Identità digitale* chiede indicazioni allo stesso utente, ad esempio, facendo scegliere il proprio gestore dell'identità digitale da un elenco riportante tutti i gestori di identità aderenti a SPID;

- 2) il *fornitore dei servizi* indirizza il soggetto *titolare dell'identità digitale* presso il *gestore dell'identità digitale*, individuato al passaggio precedente, richiedendo l'autenticazione con il livello SPID associato al servizio richiesto e l'eventuale attestazione di attributi necessari per l'autorizzazione all'accesso;

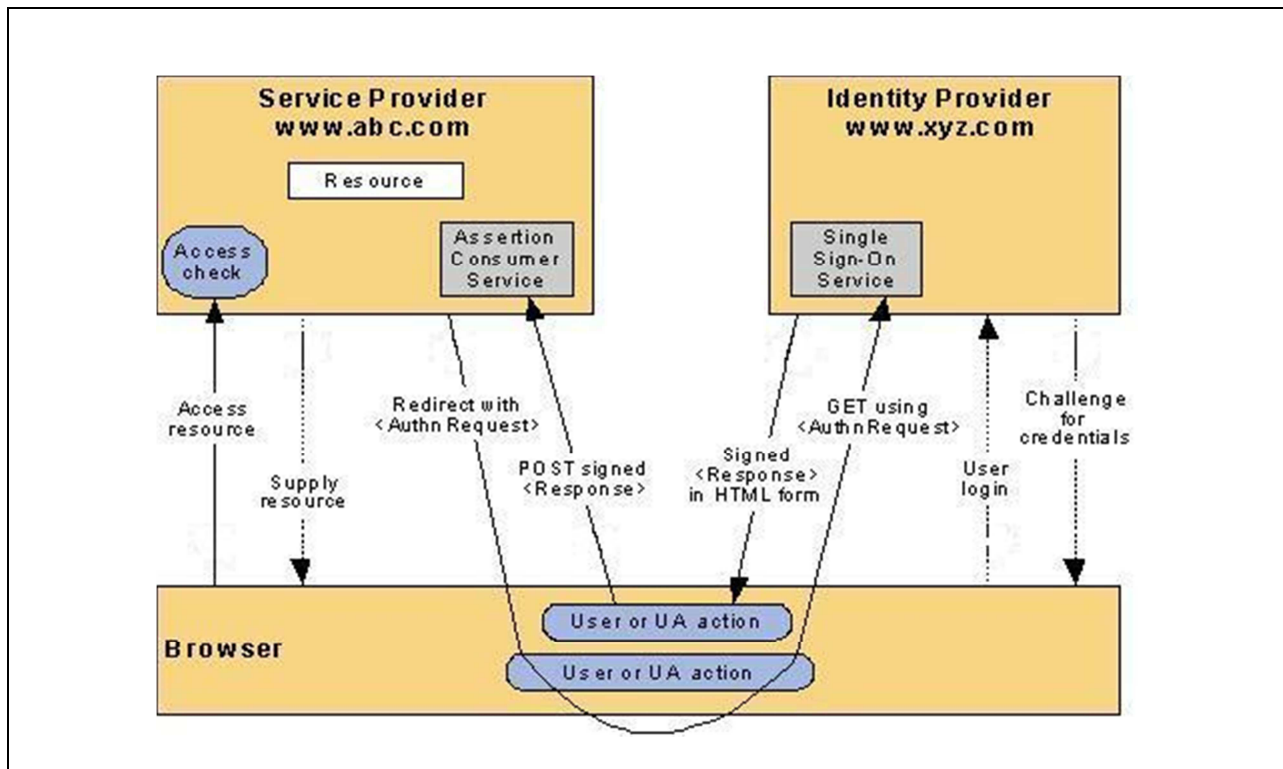


- 3) *il gestore dell'identità digitale* verifica l'identità del soggetto sulla base di credenziali fornite dallo stesso. Se tale verifica ha esito positivo viene emessa, ad uso del *fornitore dei servizi*, una asserzione di autenticazione SAML attestante gli attributi eventualmente richiesti; Le modalità per la richiesta e l'impiego degli attributi deve avvenire secondo quanto specificato al successivo art.27
- 4) *il titolare dell'identità digitale* viene quindi reindirizzato, portando con sé l'asserzione prodotta, verso il *fornitore dei servizi*;
- 5) *il fornitore dei servizi* può, a questo punto, avere la necessità di verificare attributi qualificati riferibili all'utente qualora questi fossero richiesti dalle policy di sicurezza che regolano l'accesso al servizio.

In questo caso:

- a) individuati, per il tramite del registro SPID, i gestori di attributi qualificati in grado di certificare gli attributi necessari, inoltra agli stessi una richiesta di attestazione presentando i riferimenti dell'identità digitale per la quale si richiede la verifica;
- b) il risultato della richiesta è l'emissione, da parte del gestore di attributi qualificati, di una asserzione SAML;
- 6) il fornitore dei servizi, raccolte tutte le necessarie asserzioni SAML, verifica le policy di accesso al servizio richiesto e decide se accettare o rigettare la richiesta.





### SSO SP-Initiated Redirect/POST binding

Il protocollo descritto viene realizzato secondo il profilo “Web Browser SSO” dello standard SAML, nella modalità cosiddetta “SP-Initiated” e nelle versioni “Redirect/POST binding” e “POST/POST binding”. Tale modalità prevede che il processo di autenticazione sia innescato dalla richiesta operata dall’utente, tramite il suo web browser, presso il sito del *fornitore di servizi*, il quale, a sua volta, si rivolge al gestore dell’identità inoltrando una richiesta di autenticazione SAML basata sul costrutto <AuthnRequest> e usando il binding HTTP Redirect o il binding HTTP POST.

La relativa risposta SAML, basata sul costrutto <Response>, veicolante una asserzione di autenticazione, viene restituita al richiedente tramite il binding HTTP POST.

### Art. 26 (Registro SPID)

Il *Registro SPID* contiene le informazioni relative ai soggetti aderenti a SPID e costituisce l’evidenza del cosiddetto “circolo di fiducia” (*circle of trust*) in esso stabilito.

La relazione di fiducia su cui si basa la federazione stabilita in SPID si realizza per il tramite dell’intermediazione dell’Agenzia, terza parte garante, attraverso l’adesione dei gestori dell’identità digitale, dei gestori degli attributi qualificati e dei fornitori di servizi. L’adesione a SPID costituisce l’instaurazione di una relazione di fiducia con tutti i soggetti già aderenti, accreditati dall’Agenzia, sulla base della condivisione dei livelli standard di sicurezza dichiarati e garantiti da SPID.

L’adesione al patto di fiducia tra le entità aderenti (gestori dell’identità digitale, gestori degli attributi qualificati e fornitori di servizi) si evidenzia nella presenza di tali entità nel *Registro SPID* gestito





dall'Agenzia.

La consultazione del registro consente agli aderenti a SPID di conoscere tutti i soggetti facenti parte del sistema federato e le loro caratteristiche. Le informazioni presenti sono accessibili via web sul sito dell'Agenzia e in modalità applicativa come specificato nelle regole tecniche, ai sensi di quanto previsto dall'articolo 4, comma 2 del DPCM.

#### **Art. 27**

##### *(Uso degli attributi SPID)*

I fornitori di servizi, per verificare le policy di sicurezza relativi all'accesso ai servizi da essi erogati potrebbero avere necessità di informazioni relative ad attributi riferibili ai soggetti richiedenti. Tali policy dovranno essere concepite in modo da richiedere per la verifica il set minimo di attributi pertinenti e non eccedenti le necessità effettive del servizio offerto e mantenuti per il tempo strettamente necessario alla verifica stessa, come previsto dall'articolo 11 del decreto legislativo n. 196 del 2003.

I fornitori di servizio dovranno segnalare ai gestori delle identità quali attributi identificativi e secondari dovranno essere attestati con l'asserzione emessa a seguito dell'autenticazione dei soggetti richiedenti i servizi. I gestori dell'identità, al momento dell'autenticazione e prima di emettere l'asserzione, devono ottemperare all'obbligo di informativa di cui all'articolo 13 del decreto legislativo n. 196 del 2003.

Nel caso in cui per l'applicazione delle policy di accesso relative al servizio invocato si rendesse necessaria la verifica di attributi qualificati riferibili al richiedente, i fornitori di servizio si rivolgeranno ai gestori degli attributi qualificati in grado di certificare tali attributi, individuabili attraverso il registro SPID. Per far ciò, prima di procedere, ai sensi del comma 2 dell'articolo 13 del DPCM, danno evidenza all'utente degli attributi qualificati necessari in ottemperanza all'obbligo di informativa di cui all'articolo 13 del decreto legislativo n. 196 del 2003.

#### **Art. 28**

##### *(Gestione delle sessioni di autenticazione)*

Il modello di gestione delle sessioni di autenticazione in SPID si differenzia a seconda del livello SPID con il quale viene instaurato un contesto di autenticazione.

##### *A) Gestione delle sessioni per il livello 1 SPID*

Per il livello 1 SPID è ammessa l'instaurazione di una sessione di autenticazione, associata ad un determinato utente titolare di identità digitale, mantenuta dal gestore dell'identità digitale e condivisa da tutti i fornitori di servizio che nel corso di vita della sessione stessa erogano servizi per quel determinato utente.

Per ogni nuovo fornitore di servizi che si aggiunge al contesto di autenticazione, il gestore dell'identità digitale dovrà dare informativa all'utente ai sensi dell'articolo 13 del decreto legislativo n. 196 del 2003

Il fornitore di servizi che condivide una sessione di autenticazione di un dato gestore di identità digitale, può instaurare con l'utente una sessione finalizzata al solo accesso al servizio richiesto e per questa sessione deve fornire meccanismi espliciti per il logout dell'utente.

L'utilizzo di cookies per la gestione della sessione è operato secondo le linee guida indicate dall'Autorità Garante per la protezione dei dati personali.



Per la chiusura della sessione comune è previsto un meccanismo logout globale secondo il *single logout profile* di SAML ( cfr par. 4.4 del documento *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*)

#### *B) Gestione delle sessioni per i livelli 2 e 3 SPID*

Per i livelli 2 e 3 SPID, allo scopo di garantire la massima sicurezza e stabilità del sistema, non si prevede la possibilità di mantenimento di sessioni condivise di autenticazione.

Pertanto:

- 1) il gestore dell'identità digitale non deve mantenere alcuna sessione di autenticazione con l'utente;
- 2) ogni fornitore di servizi deve gestire per proprio conto l'eventuale sessione con l'utente. Per la chiusura dovranno essere forniti meccanismi espliciti per il logout. L'utilizzo di cookies per la gestione della sessione è operato secondo le linee guida indicate dall'Autorità Garante per la protezione dei dati personali.

#### *Art.29*

##### *(Tracciatura e conservazione della documentazione di riscontro)*

Il comma 2 dell'articolo 13 del DPCM obbliga i fornitori di servizi alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi. Tali informazioni saranno costituite da registrazioni composte dal messaggio SAML di richiesta di autenticazione e della relativa asserzione emessa dal gestore delle identità. Tali messaggi riportano identificativi e date di emissione e sono firmati, rispettivamente, dallo stesso *fornitore di servizi* e dal *gestore dell'identità digitale*; quest'ultima caratteristica fornisce le necessarie garanzie di integrità e non ripudio.

L'insieme delle Registrazioni costituisce il Registro delle transazioni del fornitore del servizio. Le tracciate devono avere caratteristiche di riservatezza, inalterabilità e integrità e sono conservate adottando idonee misure di sicurezza ai sensi dell'articolo 31 del decreto legislativo 30 giugno 2003, n. 196, sotto la responsabilità del titolare del trattamento; l'accesso ai dati è riservato a personale espressamente autorizzato e incaricato del trattamento dei dati personali. Devono essere utilizzati meccanismi di cifratura.

Analogo registro dovrà essere tenuto dal gestore delle identità digitali, secondo modalità definite nelle regole tecniche Di cui all'articolo 4, comma 3 del DPCM.

Nel caso in cui uno stesso soggetto sia, allo stesso tempo, gestore dell'identità digitale e fornitore di servizi devono essere mantenute separate i distinti livelli di tracciatura delle transazioni la cui gestione deve far capo a strutture organizzative diverse.

#### *Sezione V* **Monitoraggio**



**Art. 30**  
**(Monitoraggio di AGID sul sistema SPID )**

L'Agenzia svolge funzioni di monitoraggio, anche sulla base delle segnalazioni fatte dai cittadini, allo scopo di valutare e garantire usabilità, accessibilità e corretto utilizzo degli elementi identificativi SPID e indica le migliori pratiche da adottare. Ai fini dell'attività di vigilanza, i gestori di identità digitali rendono disponibili all'Agenzia:

- 1) le informazioni circa il livello di soddisfazione dei propri clienti;
- 2) le caratteristiche di eventuali servizi aggiuntivi offerti;
- 3) le informazioni relative a disservizi, secondo la classificazione e le modalità riportate nella tabella seguente.

<b>Classificazione dei disservizi in relazione agli effetti prodotti e relativi codici identificativi</b>
1. Comportamento anomalo e non circoscritto: comportamento difforme dalle regole tecniche per il quale non è circoscritto il potenziale impatto (codice 1A, se rilevato dal gestore; codice 1B, se rilevato da terzi).
2. Comportamento anomalo circoscritto: comportamento difforme dalle regole tecniche per il quale è circoscritto il potenziale impatto (codice 2A, se rilevato dal gestore; codice 2B, se rilevato da terzi).
3. Malfunzionamento bloccante: tipologia di malfunzionamento a causa del quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, non possono essere utilizzate in tutto o in parte consistente dagli utenti (codice 3A, se rilevato dal gestore; codice 3B, se rilevato da terzi).
4. Malfunzionamento grave: tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, possono essere utilizzate parzialmente dagli utenti (codice 4A, se rilevato dal gestore; codice 4B, se rilevato da terzi).
5. Malfunzionamento: situazione a causa della quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (codice 5A, se rilevato dal gestore; codice 5B, se rilevato da terzi).

**Classificazione dei disservizi**

I gestori dell'identità digitale hanno l'obbligo di comunicare all'Agenzia, entro trenta minuti dalla rilevazione dell'evento stesso, i disservizi contraddistinti da uno dei seguenti codici: 1A, 1B, 2A, 2B, 3A, 3B ed entro due ore i disservizi contraddistinti dai codici 4A, 4B, 5A e 5B.



La comunicazione deve fornire anche una prima valutazione dell'incidente, le eventuali misure adottate al riguardo e la tempistica prevista per il ripristino della normale operatività.

A seguito delle risultanze dell'attività di monitoraggio e della rilevanza/frequenza dei disservizi, nell'ipotesi di inosservanza di uno o più degli obblighi posti a carico del gestore delle identità digitali, l'Agenzia può disporre l'inibizione all'esercizio dell'attività svolta dal gestore inadempiente, indicando nel contempo il termine entro il quale il gestore stesso deve conformarsi agli obblighi previsti. Qualora il gestore non provveda in tal senso nei tempi indicati, l'Agenzia, con provvedimento motivato notificato all'interessato, può adottare le azioni previste dall'articolo 12, comma 4 del DPCM.

I gestori delle identità digitali informano tempestivamente l'Agenzia e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali.

I gestori delle identità digitali inviano all'Agenzia, con cadenza almeno bimestrale, i dati statistici relativi all'utilizzo del sistema, le metriche quantitative e qualitative che saranno definite e concordate a valle dello *start up* di SPID.

#### *Art. 31 (Convenzioni)*

Gli schemi di convenzione per i gestori dell'identità digitale e per le pubbliche amministrazioni in qualità di fornitori di servizi sono definiti nell'ambito di specifici regolamenti emanati dall'Agenzia entro il 15 settembre 2015.

Gli schemi di convenzione per i gestori degli attributi qualificati e per i fornitori di servizi privati sono definiti nell'ambito di specifici regolamenti emanati dall'Agenzia entro il 15 dicembre 2015.



### Appendice A – Criteri per l'attribuzione dei livelli di sicurezza dei servizi

Il sistema SPID è basato su tre livelli di sicurezza di autenticazione informatica, con il livello 1 associato a quello più basso ed il livello 3 a quello più elevato. Ai sensi dell'articolo 6, comma 5 del DPCM, l'erogatore del servizio deve scegliere il livello di sicurezza da associare all'accesso del servizio stesso.

La scelta del livello di sicurezza (LoA) deve essere fondamentalmente basata sulle conseguenze derivanti da un accesso improprio a sistemi o applicazioni determinato dalla probabilità di errore che si può commettere nel processo di autenticazione; livelli di sicurezza (LoA) più alti saranno associati a servizi per i quali un accesso improprio comporta conseguenze e impatti più significativi (come sistemi che trattano dati sensibili o dati relativi a reddito o patrimonio) mentre richieste a carattere informativo possono essere associate a livelli più bassi.

E' importante evidenziare il fatto che la scelta dei livelli di sicurezza è operata a tutela degli interessi reciproci degli utenti fruitori che degli erogatori dei servizi. Ad evidenziare ciò basta riferirsi a servizi relativi a operazioni dispositive, come bonifici on line effettuati attraverso servizi di home banking. E' chiaro che se la banca, erogatrice del servizio, ha interesse a tutelarsi contro i furti on-line operati, ad esempio, attraverso furti di identità, questo interesse coincide con quello del titolare del conto corrente on-line dal quale vengono fraudolentemente sottratti i fondi.

La metodologia suggerita dall'Agenzia prevede l'identificazione dei rischi per ogni specifico servizio e la conseguente assegnazione dei livelli di sicurezza previsti in ambito SPID; ovviamente la misura dello impatto potenziale di questi rischi individuati dipende dallo specifico contesto e dalle entità coinvolte da impropria autenticazione.

La tabella seguente fornisce sinteticamente una serie di possibili associazioni

	<b>Impatto potenziale massimo di eventi per ogni livello di sicurezza SPID</b>		
<b>Impatto causato da un accesso improprio</b>	<b>Livello 1</b>	<b>Livello 2</b>	<b>Livello 3</b>
	Sistema di autenticazione a singolo fattore, discreta sicurezza sulla fedeltà/esattezza dell'identità asserita	Sistema di autenticazione a doppio fattore, alta sicurezza sulla fedeltà/esattezza dell'identità asserita	Sistema di autenticazione a doppio fattore basato su certificati digitali, elevatissima sicurezza sulla fedeltà/esattezza dell'identità asserita
Potenziale danno di reputazione	Basso	Moderato	Alto
Potenziali danni finanziari del l'utente e dell'erogatore del servizio	Basso	Moderato	Alto



Potenziale danno per rilascio di informazioni sensibili dell'utente	N/A	Basso	Moderato/Alto
Potenziale danno per violazioni di carattere civile, ad es. non conformità a regolamenti, norme ecc.	N/A	Basso/Moderato	Alto
Potenziati danni a programmi di interesse pubblico	Basso	Moderato	Alto
Impatto potenziale per la sicurezza personale dell'utente e dell'erogatore del servizio	N/A	Basso	Moderato/Alto

#### Impatto Potenziale/Livello di Sicurezza SPID

Dove per il valore (basso, moderato, alto) assegnato ai potenziali impatti è stato scelto la definizione normalmente adottata nell' ISO/IEC 27001 framework e FIPS 199.

Valore Impatto	
Basso	La perdita di confidenzialità, integrità e disponibilità ha un effetto negativo limitato per l'operatività delle organizzazioni, per i beni e per le persone.
Moderato	La perdita di confidenzialità, integrità e disponibilità potrebbe avere un serio effetto negativo per l'operatività delle organizzazioni, per i beni e per le persone.
Alto	La perdita di confidenzialità, integrità e disponibilità potrebbe avere un severo o catastrofico effetto negativo per l'operatività delle organizzazioni, per i beni e per le persone.

#### Definizione valore impatto

Ulteriori considerazioni possono essere fatte in relazione alla classificazione dei dati secondo lo schema riportato in tabella, fermo restando la facoltà della singola Amministrazione di definire criteri diversi in base alle diverse modalità di erogazione dei servizi e ai dati resi disponibili :

Livello	Classificazione	Tipo di accesso	Esempi
---------	-----------------	-----------------	--------



	del dato		
<b>nessuno</b>	Pubblico	Non è richiesto nessun livello di autenticazione.	Esempio area informativa del sito <a href="http://www.agid.gov.it">www.agid.gov.it</a> ; <a href="http://www.comune.milano.it">www.comune.milano.it</a>
<b>1</b>	Pubblico/Interno	Livello 1 è adeguato per utenti sono iscritti ad un sito ma senza la possibilità di eseguire operazioni dispositive.	Esempio 1. area cittadini ma non dispositiva del comune di Roma <a href="https://www.comune.roma.it/wps/myportal">https://www.comune.roma.it/wps/myportal</a>
<b>2</b>	Interno	Livello 2 è adeguato per utenti che accedono ad informazioni che hanno creato, o per utenti che per motivazioni professionali possono ad trattare informazioni di soggetti terzi.	Esempio area riservata dei comuni per il pagamento di tasse e tributi, inoltre di richieste/domande, interrogazioni, aggiornamenti e cancellazioni che non riguardano dati sensibili.
<b>3</b>	Riservato	Livello 3 è necessario per utenti che sulla base di ruoli/responsabilità possono accedere ad informazioni di tipo riservato.	Esempio siti che trattano dati sensibili, specifiche transazioni che includono trasferimento di fondi, accesso a documenti riservati o rilevanti per le amministrazioni e le imprese.

#### Classificazione dato/Tipo di accesso

L'Agenzia, al fine di rendere omogenei i LoA associati ai servizi su tutto il territorio nazionale, promuove e pubblica, nella sezione SPID del proprio sito istituzionale il LoA da associare alle categorie di servizi che presentano carattere di omogeneità.



**Appendice B – Minacce associate alla gestione del ciclo di vita delle identità digitali**  
**Minacce per il processo verifica dell'identità dichiarata in fase di registrazione.**

In generale sussistono due categorie di minacce nel processo di registrazione:

- a) furto/usurpazione di identità
- b) compromissione o uso non corretto della infrastruttura associata ai servizi erogati dal gestore delle identità digitali. Questa problematica rientra in quella generale relativa ai controlli di sicurezza (separazione dei compiti, conservazione della documentazione, audit indipendenti)

La tabella A elenca le minacce correlate al processo di registrazione.

Attività	Minaccia/Attacco	Esempio
Registrazione	Furto/usurpazione di identità	Un richiedente dichiara una identità non corretta ad es. usando un documento d'identità contraffatto
	Ripudio/disconoscimento della registrazione	Un cittadino/impresa nega la registrazione affermando che non ha mai richiesto la registrazione

**Minacce nel processo di registrazione**

Le minacce di registrazione possono essere impedito, o almeno dissuase, rendendo più complessa la possibilità di effettuare un furto di identità e aumentando la probabilità di rilevazione di queste evenienze.

A qualsiasi livello devono essere utilizzati dei metodi (1) per verificare l'esistenza di una persona con l'identità dichiarata, (2) che il richiedente sia effettivamente l'utente titolare dell'identità dichiarata e (3) che lo stesso non può successivamente disconoscere la registrazione.

*Minacce associate al processo di emissione delle credenziali*

Le minacce nel processo di emissione riguardano attacchi causati da furti/usurpazione di identità e da meccanismi di trasporto per l'emissione delle credenziali.

La tabella elenca le minacce ed esempi di possibile strategia di mitigazione correlate al processo di emissione.





Attività	Minaccia/Attacco	Esempio	Strategia di mitigazione
Emissione	Divulgazione/rivelazione	Una chiave generata dal gestore delle identità digitali è copiata da un aggressore informatico.	Emissione delle credenziali di persona, spedizione in buste sigillate con posta raccomandata, uso di una sessione protetta per la spedizione in modalità elettronica
	Manomissione	Una nuova password generata dal sottoscrittore viene modificata da un aggressore informatico.	Emissione delle credenziali di persona, spedizione in buste sigillate con posta raccomandata, uso di protocolli di comunicazione che proteggono la sessione dati.
	Emissione non autorizzata	Rilascio delle credenziale ad una persona che afferma di essere il sottoscrittore (e in effetti non lo è)	Definizione di una procedura che assicura che la persona destinataria delle credenziali sia la stessa persona che ha partecipato nel processo di registrazione

#### Minacce/Processo di emissione

##### *Minacce associate ai token*

Un potenziale aggressore malevolo può prendere il controllo di un token e fingere di essere il legittimo proprietario del token. Le minacce associate ai token sono classificate in base alla tipologia dei token:



Tipo token	Esempi di minacce
Qualcosa che abbiamo	Può essere perso, danneggiato, rubato o clonato. Ad esempio un aggressore malevolo potrebbe prendere possesso del computer e copiare un token software. Analogamente un token hardware potrebbe essere rubato, manomesso o duplicato.
Qualcosa che conosciamo	L'aggressore potrebbe provare ad indovinare la password o il PIN o installare del software maligno (ad es. keyboard logger) per catturare la password, in alternativa possono essere adottate catture del traffico dalla rete o attraverso tecniche di social engineering
Qualcosa che siamo	Può essere replicato, ad esempio un aggressore potrebbe ottenere una copia delle impronte digitali e costruirne una replica assumendo che il sistema biometrico non utilizzi robuste, e consigliate, tecniche di rilevazione.

#### Tipo token

La tabella che segue illustra le minacce/attacchi più comuni:

Minaccia/Attacco token	Descrizione	Esempi
Furto	Un token fisico viene rubato	Furto di un cellulare, dispositivo fisico ecc.
Scoperta	Le risposte a domande di suggerimento per riconoscere l'utente sono facilmente deducibili o ricavabili da diverse sorgenti disponibili.	Ad es. la domanda "Quale liceo hai frequentato ?" è facilmente ottenibile dai siti web di tipo social.
Duplicazione	Il token è stato copiato senza , o con, l'assenso dell'utente.	Password scritta su post-it o memorizzato su un file che viene successivamente copiato da un aggressore.
Intercettazione	Il token viene rilevato nel momento dell'immissione.	La password viene dedotta osservando l'immissione da tastiera, o con l'ausilio di keylogger software.



Offline cracking	Sono usate tecniche analitiche offline ed esterne ai meccanismi di autenticazione.	Una chiave viene estratta utilizzando tecniche di analisi differenziale su token hardware rubati. Un token software PKI può essere soggetto ad attacchi da dizionario per identificare la password corretta da usare per decifrare la chiave privata.
Phishing o pharming	L'utente viene ingannato e crede che l'aggressore sia il fornitore di servizi o di identità (sito civetta).	DNS re-routing. Una password viene rivelata ad un sito civetta che simula l'originale.
Ingegneria sociale	L'aggressore stabilisce un livello di sicurezza con l'utente in modo da convincerlo a rivelargli il contenuto del token.	Una password viene rivelata durante una telefonata ad un aggressore che finge di essere l'amministratore di sistema.
Provare a indovinare (online)	L'aggressore si connette al sito del gestore di identità online e prova ad indovinare il token valido.	Attacchi online basati su dizionari o password note.

**Minacce/Tipo token**

E le strategie di mitigazione delle minacce sono indicate nella tabella.

<b>Minaccia/Attacco token</b>	<b>Tecnica di mitigazione della minaccia</b>
Furto	usare token multi-fattore che devono essere attivati attraverso un PIN o elementi biometrici.
Scoperta	Usare metodologie tali da rendere complessa la deduzione di una risposta
Duplicazione	Usare token difficilmente duplicabili come token crittografici hardware.
Intercettazione	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.
Offline cracking	Usare token con elevata entropia. Usare token che causino il blocco dopo un numero limitato di tentativi.



Phishing o pharming	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.
Ingegneria sociale	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.
Provare a indovinare (online)	Usare token con elevata entropia. Usare token che causino il blocco dopo un numero limitato di tentativi.

**Tipo minaccia/Tecnica di mitigazione**

A queste tecniche possono essere applicate strategie addizionali come l'uso di fattori multipli, meccanismi di sicurezza fisica, regole di complessità sulle password, sistematici controlli di sicurezza sulla rete e sui sistemi, tecniche out of band per la verifica del possesso di dispositivi registrati, addestramento periodico e informazione preventiva u potenziali minacce.



### *Appendice C - Tipi di token e loro Tassonomia*

Per le credenziali a doppio fattore viene normalmente utilizzato un token di tipo hardware o di tipo software.

- Token di tipo hardware: sotto forma di dispositivo elettronico portatile di piccole dimensioni, alimentato a batteria con autonomia nell'ordine di qualche anno, dotato di uno schermo e talvolta di una tastiera numerica (alcuni token possono essere collegati ad un computer tramite una porta USB per facilitare lo scambio di dati).
- Token di tipo software: le informazioni necessarie risiedono direttamente nell'apparato dell'utente (PC, tablet, ecc.), e non in un oggetto esterno.

In particolare nei token crittografici multi-fattore, una chiave crittografica viene direttamente contenuta nel dispositivo hardware o viene immagazzinata su un disco, o equivalente media “soft”, nel caso di token software ne viene richiesta l'attivazione attraverso un secondo fattore di autenticazione. L'autenticazione, in questo caso, è ottenuta provando sia il possesso che il controllo della chiave. Il convalidatore del token dipende strettamente dallo specifico protocollo crittografico, generalmente basato su qualche tipo di messaggio firmato, ad esempio, nel caso del protocollo TLS, è previsto il messaggio di “certificate verify”.

I token del tipo one-time password (OTP) multi-fattore, sono dispositivi hardware che generano una password valida una sola volta nella fase di attivazione e che richiedono l'attivazione attraverso un secondo fattore di autenticazione. Il secondo fattore di autenticazione può essere ottenuto attraverso “qualcosa che conosciamo” ad es. un PIN o “qualcosa che siamo” ad esempio attraverso la lettura di elementi biometrici (impronte digitali). La password one-time viene normalmente visualizzata sul dispositivo e deve essere digitata manualmente (in alcuni casi può essere prevista la lettura diretta dal computer attraverso, ad esempio, l'interfaccia USB).

Per completezza, i processi di autenticazione multi-stadio nel quale viene utilizzato un token a singolo fattore per ottenere un secondo token non costituiscono una vera autenticazione multi-fattore, in questo caso il livello di sicurezza dell'autenticazione della soluzione combinata è pari a quello del token più debole. Ad esempio, alcune soluzioni in mobilità si basano su chiavi crittografiche complete o parziali memorizzate su un server online e scaricate sul computer locale del richiedente dopo una prima autenticazione basata sull'uso di password. Successivamente, il richiedente può usare il token crittografico precedentemente scaricato per autenticarsi con un gestore di identità remoto; questo tipo di soluzione deve essere considerata dello stesso livello di sicurezza della password usata dal richiedente per ottenere il token crittografico.

In alcuni casi può essere preferibile elevare il livello di sicurezza dell'autenticazione durante una sessione applicativa, ciò può essere considerato un caso speciale di autenticazione multi-token dove un primo token (ad es. la password) viene utilizzato per stabilire una sessione sicura ed un secondo token (ad es. un out of band token) viene utilizzato per attivare una particolare transazione durante la sessione. Anche se i due token sono usati in fasi differenti, viene normalmente riconosciuto questo risultato come uno schema di autenticazione multi-token che può elevare il livello globale di sicurezza dell'autenticazione se i due token appartengono a due tipologie (“che abbiamo”, “che conosciamo”, “che siamo”) differenti.



Di seguito si descrivono i principali tipi di token utilizzabili per l'autenticazione informatica:

- **Token con segreto memorizzato:** tipicamente è composto da una stringa di caratteri (password) o una sequenza di cifre (PIN); nel caso SPID per essere considerato a livello 1 di sicurezza di autenticazione informatica devono essere rispettate le caratteristiche, policy e regole di complessità delle password indicate al paragrafo relativo alla creazione delle credenziali.
- **Token con conoscenza pre-registrata:** normalmente una serie di richieste o indicazioni (prompt o challenge) che vengono stabilite tra l'utente e il gestore delle identità digitali durante la fase di registrazione (ad es. una risposta del tipo "il nome di tua da nubile ?").
- **Token con tabella dei codici/segrete:** un token fisico o elettronico che contiene una tabella di codici riservati, all'utente può essere richiesto di rispondere con il codice/segreto corrispondente ad una specifica posizione della tabella.
- **Token out of band:** un token fisico indirizzabile in modo univoco che può ricevere un codice/segreto selezionato dal gestore dell'identità per essere usato una sola volta durante la sessione di servizio (ad esempio un codice inviato via SMS ad un numero di cellulare certificato).
- **Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP):** un dispositivo hardware che supporta la generazione automatica di una OTP (ad es. un codice composto da sei caratteri).
- **Dispositivo Crittografico a singolo fattore (SF):** un dispositivo hardware che esegue operazioni crittografiche su un input al dispositivo. Il dispositivo non richiede l'attivazione attraverso un secondo fattore di autenticazione. Questo dispositivo usa chiavi crittografiche asimmetriche o simmetriche embedded (integrate nel dispositivo stesso).
- **Token crittografico software multi-fattore (MF):** una chiave crittografica è memorizzata su un disco o un altro "media" e richiede l'attivazione attraverso un secondo fattore di autenticazione. L'autenticazione viene quindi ottenuta provando il possesso e il controllo della chiave. Questo sistema è basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell' Allegato 3 della Direttiva 1999/93/CE
- **Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP):** un dispositivo hardware che genera una one-time password per l'uso durante l'autenticazione e che richiede l'attivazione attraverso un secondo fattore di autenticazione (ad es. un dato biometrico, un dato digitato su un pad integrato ecc.)
- **Dispositivo Crittografico multi-fattore (MF):** un dispositivo hardware che contiene chiavi crittografiche che richiedono l'attivazione attraverso un secondo fattore di autenticazione. L'autenticazione viene quindi ottenuta provando il possesso e il controllo della chiave. Questo sistema è basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell' Allegato 3 della Direttiva 1999/93/CE.



### Appendice D – Usabilità e Accessibilità

Per lo sviluppo dell'interfaccia utente, i fornitori di servizi e i gestori delle identità digitali devono garantire:

- l'usabilità ovvero la facilità d'uso come
  - la presentazione delle informazioni e delle scelte in modo chiaro e conciso, la mancanza di ambiguità e il posizionamento di elementi importanti in aree appropriate
  - la garanzia del funzionamento su diversi dispositivi e browser secondo lo stato dell'arte della tecnologia.
- l'accessibilità per tutelare il diritto di accesso ai servizi informatici e telematici della pubblica amministrazione da parte dei disabili in coerenza con Legge n. 4 del 9 gennaio 2004, aggiornato dal DM 20 marzo 2013, e le indicazioni Web Accessibility Initiative (WAI) del World Wide Web Consortium (W3C).

Al fine di ricondurre a una user experience comune per tutti gli utenti, limitandone l'eventuale disorientamento nell'accesso tramite diversi gestori dell'identità digitale, l'interfaccia del percorso di iscrizione (sign up) presso i gestori di identità digitale, nonché del login per l'accesso ai fornitori di servizi, sarà unica per tutti i gestori, fatto salvo lo spazio predisposto per la visualizzazione del proprio logo.

Nella sezione SPID del sito AgID saranno pubblicati tutti gli aggiornamenti e le ulteriori indicazioni al fine di garantire una omogenea user experience.

#### D.1 Richiesta identità SPID

Accedendo al sito di un fornitore di servizi aderente a SPID o al sito italia.it è permesso, ad un utente non ancora registrato, di acquisire una identità SPID. All'utente sarà sottoposta la scelta del gestore dell'identità, tra i diversi disponibili, presso cui richiedere l'attivazione della propria identità digitale – figura D1 -. Una volta operata tale scelta l'utente verrà instradato verso il gestore prescelto. In alternativa l'utente può autonomamente collegarsi direttamente al sito del gestore di sua preferenza e selezionare la pagina di Richiesta identità SPID.



Figura D1. Finestra selezione gestore presso il fornitore dei servizi

Qualunque sia il percorso seguito l'utente accederà a questo punto alla pagina di inizio della procedura di registrazione che riporterà l'indicazione del numero di passaggi necessari a concludere il processo e l'interfaccia d'inserimento dei campi obbligati dell'identificativo utente, della password e della mail. La pagina - figura D2 - conterrà inoltre le indicazioni sul tempo e i documenti necessari per la registrazione. Da questa pagina si potrà anche accedere alla procedura di registrazione semplificata, nel caso l'utente sia già provvisto di un profilo presso lo stesso gestore di identità.

Figura D2. Finestra di inserimento dati di accesso

Ogni singolo passaggio di inserimento dati da parte dell'utente avrà un suo aiuto contestuale. Al momento dell'inserimento della propria mail si avrà la possibilità (non obbligatoria) di attivarne una presso il gestore dell'identità digitale.

Figura D3. Finestra di inserimento mail

L'inserimento della password sarà a discrezione dell'utente, indicando un minimo di 8 caratteri di cui almeno una lettera maiuscola e un carattere numerico. Sarà presente un indicatore della sicurezza della password prescelta e la possibilità di generarla in maniera casuale. Sarà indicata in 180 giorni la validità della password inserita.





Figura D4. Finestra di inserimento password

Una volta inserita mail e password si riceverà l'avviso di verifica in corso e l'indicazione di seguire il link inviato su ciascuna mail indicata per procedere al passo successivo.

Figura D5. Finestra di verifica mail

La verifica della mail permetterà di procedere al secondo passo - figure D6 D 7 e D8 -, relativo all'inserimento e alla verifica del numero di un telefono cellulare.





STEP 2 SU 5

La tua email di accesso è stata verificata, grazie!

Benvenuto **mario.rossi@idp-email.it**  
per la sicurezza\* dei tuoi dati **devi avere:**

un numero di cellulare

VERIFICALO →

[\\* approfondisci](#)

Figura D6. Finestra di inserimento numero cellulare



Abbiamo appena inviato un SMS al numero **555222111** con il tuo codice di verifica a 7 cifre. Dovresti riceverlo tra alcuni istanti. Devi verificare il numero per continuare.

Inserisci il tuo codice di verifica in questo spazio

1212444

Non hai ricevuto il codice?

RICEVI SMS RICEVI TELEFONATA

← INDIETRO PROCEDI →

Figura D7. Finestra di inserimento codice

Il processo di iscrizione manca, a questo punto, dell'identificazione personale, ma il gestore dell'identità digitale dovrà già rendere utilizzabili le credenziali verificate (mail, password, cellulare), per un arco di tempo di 30 giorni, al fine di non richiedere, in un successivo accesso da parte dell'utente per il completamento della procedura, quanto precedentemente già inserito.



Il tuo numero di telefono  
è stato verificato, grazie!

Perfetto **mario.rossi@email.it**  
**il tuo accesso è quasi pronto.**  
Per attivarne i servizi devi completare la registrazione  
e farti riconoscere...

**COMPLETA ORA →**

**Tempo necessario per completare la registrazione:**  
circa 7 minuti

**Devi aver a portata di mano:**  
i tuoi dati e un documento di riconoscimento.  
In alcuni casi potrebbe essere necessario  
presentarsi nei nostri uffici (dell'IdP)  
per attivare le credenziali di accesso

Figura D8. Finestra di conferma numero di telefono

Il terzo passo - figura D9 -, prevede l'inserimento dei dati personali;

**STEP 3 SU 5**  
• • • • •

Il tuo profilo personale:

Nome      Cognome

Data di nascita      Luogo di nascita

Codice fiscale

Indirizzo di residenza

**DOCUMENTO DI IDENTITÀ →**

Figura D9. Inserimento dati anagrafici



Il quarto passo - figure D10 e D11 -, prevede l'inserimento dei dati del documento di riconoscimento (selezionabile fra l'elenco dei documenti ammessi) e l'invio, tramite upload o webcam, dell'immagine dello stesso.

Figura D10. Selezione documento d'identità

Figura D11. Inserimento documento d'identità

Il quinto e ultimo passo - figura D12 -, prevede il riepilogo dei dati, l'accettazione delle condizioni d'uso e della privacy, e la selezione della modalità con cui procedere all'identificazione personale.

Il gestore dell'identità digitale deve prevedere l'utilizzo di un sistema di identificazione digitale e almeno altre due modalità alternative a propria discrezione. Sarà importante indicare l'eventuale lasso di tempo necessario per l'attivazione dell'identità digitale dal momento del riconoscimento personale.



**STEP 5 SU 5**  
.....

**{Riepilogo dei dati inseriti}**

☐ ☐

Accettazione delle condizioni d'uso  
e della privacy policy.

Scarica PDF precompilato dell'adesione come promemoria.

Per concludere la creazione della tua identità digitale  
abbiamo bisogno di riconoscerti senza ombra di dubbio, come vuoi procedere?

Usa la tua identità digitale - Carta Identità Elettronica - Carta Nazionale Servizi - Firma Elettronica...	Prenota una conversazione webcam con un nostro operatore	Prendi un appuntamento e presentati alla nostra sede (IdP) più vicina	...
---	--	---	-----

Figura D12. Riepilogo dati inseriti

L'utente che conclude il processo di iscrizione con il riconoscimento personale acquisisce le credenziali per accedere ai servizi forniti con livelli di sicurezza SPID 1 e SPID 2.

Al momento dell'attivazione delle credenziali il gestore delle identità comunicherà la cosa all'utente congiuntamente al riepilogo dei dati, alle credenziali d'accesso, alle informazioni utili al corretto utilizzo dell'identità e alla modalità per procedere all'attivazione del successivo livello di sicurezza (SPID 3).



## D.2 Accesso ai servizi

Un utente già provvisto delle credenziali attivate accede al sito del fornitore dei servizi e cliccando il bottone “Entra con Italia.it” avvia il processo di autenticazione.



Figura D13. Sito del fornitore dei servizi

Il fornitore di servizi per individuare il gestore dell'identità in grado di autenticare l'utente potrà chiedere l'informazione direttamente all'utente. Presentando all'utente stesso la schermata descritta in figura D13 per mezzo della quale tale indicazione può essere fornita.





Figura D14. Fornitore dei servizi

Una volta individuato il gestore delle identità in grado di autenticare l'utente, quest'ultimo verrà indirizzato verso il gestore individuato presso il quale accederà alla schermata di login, che sarà già impostata per richiedere il livello di sicurezza SPID e gli attributi necessari.

Nel caso di accesso con livello di sicurezza SPID 1 sarà richiesto l'inserimento di mail e password come descritto in figura D14.

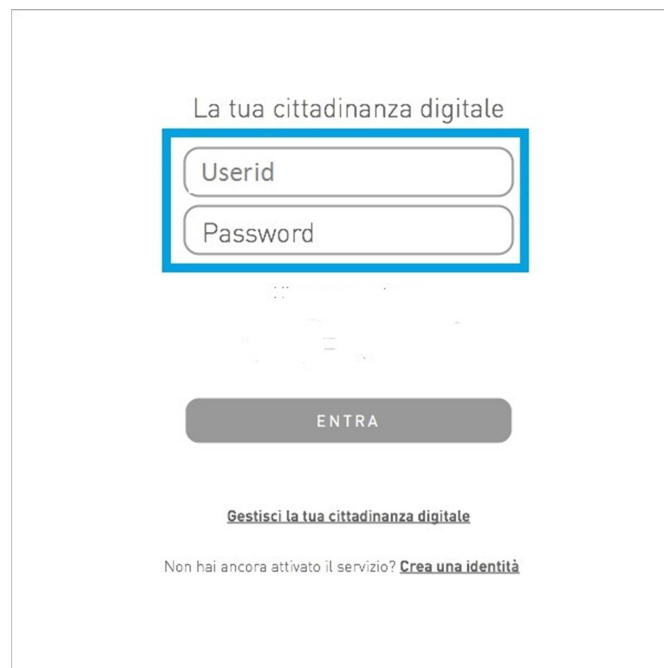


Figura D15. Finestra di login SPID



Nel caso di accesso con livello di sicurezza SPID 2 sarà richiesto l'inserimento di mail, password e del codice OTP previsto, come descritto in figura D16.

La tua cittadinanza digitale

Userid

Password

OTP

ENTRA

[Gestisci la tua cittadinanza digitale](#)

Non hai ancora attivato il servizio? [Crea una identità](#)

Figura D16. Finestra di login SPID2





### *Appendice E – Disciplina sull'utilizzo degli elementi grafici identificativi dello SPID*

Per la descrizione dettagliata dell'utilizzo degli elementi identificati dell'immagine coordinata SPID si rimanda al Manuale d'uso.

Gli elementi identificativi SPID sono costituiti da:

- logo  
palette colori  
caratteri tipografici  
griglie di impaginazione  
elementi iconografici

#### **Logo**

Il sistema del logo è composto, nella versione estesa, da un logogramma che riporta la denominazione del progetto coincidente con lo stesso dominio e URL: [italia.it](https://italia.it)



Il sistema del logo è composto, nella versione estesa, da un logogramma che riporta la denominazione del progetto coincidente con lo stesso dominio e URL: [italia.it](https://italia.it)

Del logo è disponibile una versione sintetica che riprende le iniziali e il suffisso della denominazione: .id.



#### **Palette colori**

I colori istituzionali sono rappresentati dalla coppia di blu definiti dai valori RGB  
0.102.204 (#0066CC)  
0.51.153 (#003399)



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

**Caratteri tipografici**

Il carattere tipografico istituzionale per la composizione dei testi nei siti web dei servizi SPID è il Titillium Web. Carattere disponibile come web font gratuita su Google font, all'indirizzo

<http://www.google.com/fonts/specimen/Titillium+Web>

<http://www.google.com/fonts#UsePlace:use/Collection:Titillium+Web>

**Titillium Web Leggero**

Abcdefghijklmnopqrstuvwxyz1234567890

ABCDEFGHIJKLMNOPQRSTUVWXYZ1234

**Titillium Web Regolare**

Abcdefghijklmnopqrstuvwxyz1234567890

ABCDEFGHIJKLMNOPQRSTUVWXYZ1234

**Titillium Web Grassetto**

Abcdefghijklmnopqrstuvwxyz1234567890

ABCDEFGHIJKLMNOPQRSTUVWXYZ1234

Di seguito alcune versioni di fogli stile utilizzabili nel rapporto titolo/testo.

Titillium Web Grassetto c. 48/54

Titillium Web Regolare c. 24/30

# Titolo 48px

Lorem ipsum dolor sit amet, per laoreet  
delicatissimi in, rebum meliore menandri  
et usu, ea nemore iudicabit has.

Titillium Web Grassetto c. 36/44

Titillium Web Regolare c. 18/24



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

# Titolo 36px

Lorem ipsum dolor sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabitm dolor sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabit has.

Titillium Web Grassetto c. 24/30

Titillium Web Regolare c. 14/18

## Titolo 24px

Lorem ipsum dolor sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabitm dolor sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabit sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabitm dolor sit amet, per laoreet delicatissimi in, rebum meliore menandri et usu, ea nemore iudicabit has has.

### Griglie di impaginazione

Qualsiasi utilizzo del logo dovrà prevedere uno spazio di rispetto.



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

### Elementi iconografici

Un set di elementi iconografici (bottoni, testate, pittogrammi) completa il sistema di identità. Gli elementi saranno disponibili in diversi formati.





## **REGOLAMENTO**

### **RECANTE LE REGOLE TECNICHE (articolo 4, comma 2, DPCM 24 ottobre 2014)**

**Visto** il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale, e, in particolare, l'articolo 64 che prevede l'istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese” (di seguito: SPID);

**Visto** il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 che definisce le caratteristiche di SPID, nonché i tempi e le modalità di adozione dello stesso da parte delle pubbliche amministrazioni e delle imprese, e, in particolare, l'articolo 4, comma 2;

**Visto** il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

**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 e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta ufficiale dell'Unione europea serie L 257 del 28 agosto 2014;

**Sentito** il Garante per la protezione dei dati personali;

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

## 1 REGOLE TECNICHE PER IL GESTORE DELL'IDENTITÀ DIGITALE

Le modalità di funzionamento del *Gestore dell'identità digitale*, nel seguito indicato anche con il termine tecnico *Identity provider*, dovranno essere quelle previste da SAML v2 per il profilo “*Web Browser SSO*” (cfr. [SAML-TechOv] sez. 4.1)

Devono essere previste le due versioni “*SP-Initiated*”: “*Redirect/POST binding*” e “*POST/POST binding*”, in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo *User Agent*) ad un *fornitore di servizi*, nel seguito indicato anche con il termine tecnico *Service Provider*, il quale a sua volta si rivolge all'*Identity provider* opportuno in modalità “pull”.

La richiesta di autenticazione SAML (basata sul costrutto <**AuthnRequest**>) può essere inoltrata da un *Service Provider* all'*Identity Provider* usando il *binding HTTP Redirect* o il *binding HTTP POST*.

La relativa risposta SAML (basata sul costrutto <**Response**>) può invece essere inviata dall'*Identity Provider* al *Service Provider* solo tramite il *binding HTTP POST*.

Interfacce logiche dell'*Identity Provider* coinvolte:

- **IIDPUserInterface**: permette agli utenti l'interazione via web con il componente tramite *User Agent* in fase di challenge di autenticazione;
- **IAuthnRequest (singleSignOnService)**: ricezione di richieste di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei SAML *metadata* dell'*Identity Provider*

Interfacce logiche del *Service Provider* coinvolte:

- **IAuthnResponse (Assertion Consumer Service)**: ricezione delle risposte di autenticazione SAML.
- **IMetadataRetrieve**: permette il reperimento dei SAML *metadata* del *Service Provider*
- **IDSResponse**: ricezione delle risposte da parte del *Discovery Service*.

### 1.1. SCENARIO DI INTERAZIONE IN MODALITÀ SSO

Lo scenario completo è quello illustrato in Figura 1 - SSO SP-Initiated Redirect/POST binding nel caso di *SP-Initiated - Redirect/POST binding* e descritto dalla Tabella 1 - SSO SP-Initiated Redirect/POST binding.



	Descrizione	Interfaccia	SAML	Binding
1	Il fruitore utilizzando il browser (User Agent) richiede l'accesso alla risorsa			
2a	Il Service Provider (SP) invia allo User Agent (UA) una richiesta di autenticazione da far pervenire all'Identity Provider (IdP).	IAuthnRequest	AuthnRequest	HTTP Redirect HTTP POST
2b	Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider.	-	AuthnRequest	HTTP Redirect HTTP POST
3	L'Identity Provider esamina la richiesta ricevuta e se necessario esegue una challenge di autenticazione con l'utente.	-	-	HTTP
4	L'Identity Provider portata a buon fine l'autenticazione effettua lo user login e prepara l'asserzione contenente lo statement di autenticazione dell'utente destinato al Service Provider (più eventuali statement di attributo emessi dall'Identity Provider stesso).	-	-	-
5	L'Identity Provider restituisce allo User Agent la <Response> SAML contenente l'asserzione preparata al punto precedente.	-	Response	HTTP POST
6	Lo User Agent inoltra al Service Provider (SP) la <Response> SAML emessa dall'Identity Provider.	IAuthnResponse	Response	HTTP POST

Tabella 1 - SSO SP-Initiated Redirect/POST binding



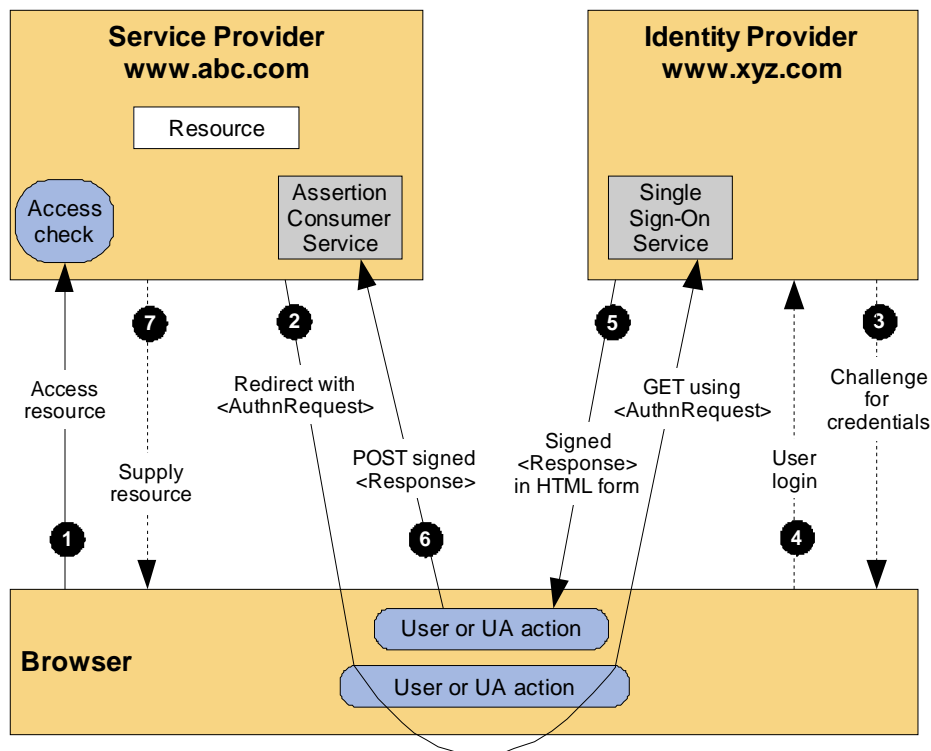


Figura 1 - SSO SP-Initiated Redirect/POST binding

## 1.2. SPECIFICHE DELLE INTERFACCE

Di seguito vengono espone le specifiche delle interfacce del *Identity Provider* riportanti:

- le caratteristiche dell'*asserzione* prodotta;
- le caratteristiche delle *AuthnRequest* e della relativa *Response*;
- le caratteristiche del *binding*;
- i *metadati*.

### 1.2.1. CARATTERISTICHE DELLE ASSEZIONI

L'*asserzione* prodotta dall'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

L'*asserzione* deve avere le seguenti caratteristiche:





- nell'elemento **<Assertion>** devono essere presenti i seguenti attributi:
  - l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
  - l'attributo **IssueInstant** a indicare l'istante di emissione della richiesta, in formato UTC (esempio: "2008-03-13T18:04:15.531Z");
- deve essere presente l'elemento **<Subject>** a referenziare il soggetto che si è autenticato in cui devono comparire:
  - l'elemento **<NameID>** atto a qualificare il soggetto dell'asserzione, in cui sono presenti i seguenti attributi:
    - **Format** che deve assumere il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*" (cfr. SAMLCore, sez. 8.3);
    - **NameQualifier** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Identity Provider* stesso);
  - l'elemento **<SubjectConfirmation>** contenente l'attributo
    - **Method** riportante il valore "*urn:oasis:names:tc:SAML:2.0:cm:bearer*"
 e l'elemento:
    - **<SubjectConfirmationData>** riportante gli attributi:
      - **Recipient** riportante l'*AssertionConsumerServiceURL* relativa al servizio per cui è stata emessa l'asserzione e l'attributo
      - **NotOnOrAfter** che limita la finestra di tempo durante la quale l'asserzione può essere propagata.
      - **InResponseTo**, il cui valore deve fare riferimento all'ID della richiesta;
- deve essere presente l'elemento **<Issuer>** a indicare l'*entityID* dell'*Identity Provider* emittente (attualizzato come l'attributo **entityID** presente nei corrispondenti IdP *metadata*) con l'attributo **Format** riportante il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";
- deve essere presente l'elemento **<Conditions>** in cui devono essere presenti gli attributi:
  - **NotBefore**,
  - **NotOnOrAfter**);
 e l'elemento:

- **<AudienceRestriction>** riportante a sua volta l'elemento **<Audience>** attualizzato con l'*entityID* del *ServiceProvider* per il quale l'asserzione è emessa;
- deve essere presente l'elemento **<AuthStatement>** a sua volta contenente l'elemento:
  - **<AuthnContext>** riportante nel sotto elemento **<AuthnContextClassRef>** la classe relativa all'effettivo contesto di autenticazione (es. *urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1*);
- può essere presente l'elemento **<AttributeStatement>** riportante gli attributi identificativi certificati dall'*Identity provider*. Tale elemento se presente dovrà comprendere:
  - uno o più elementi di tipo **<Attribute>** relativi ad attributi che l'*Identity Provider* può rilasciare (cfr. Tabella attributi SPID) su richiesta del *Service Provider* espressa attraverso l'attributo ***AttributeConsumingServiceIndex*** quando presente nella *authnrequest*;
  - per gli elementi **<AttributeValue>** si raccomanda l'uso dell'attributo ***xsi:type*** attualizzato come specificato nella Tabella attributi SPID;
- deve essere presente l'elemento **<Signature>** riportante la firma sull'asserzione apposta dall'*Identity Provider* emittente. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- può essere presente un elemento **<Advice>**, contenente a sua volta altri elementi **<Assertion>**. La possibile presenza dell'elemento, prevista per futuri usi, consente, nei casi in cui gli statement emessi dall'*Identity Provider* si basino su altre asserzioni SAML ottenute da altre authority, di fornire evidenza delle stesse in forma originale unitamente alla risposta alla richiesta di autenticazione.

**L'elemento <Advice> è previsto per futuri usi ed al momento non deve essere utilizzato.**



```

<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_27e00421b56a5aa5b73329240ce3bb832caa"
  IssueInstant="2015-01-29T10:01:03Z"
  Version="2.0" >
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">spididp.it</saml:Issuer>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        NameQualifier="http://spididp.spididpProvider.it">_06e983facd7cd554cfe067e
      </saml:NameID>
      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
          Recipient="https://spidSP.serviceProvider.it/Location_0"
          NotOnOrAfter="2001-12-31T12:00:00"
          InResponseTo="_4d38c302617b5bf98951e65b4cf304711e2166df20">
        </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-01-29T10:00:33Z" NotOnOrAfter="2015-01-29T10:02:33Z">
      <saml:AudienceRestriction>
        <saml:Audience>
          https://spidSP.serviceProvider.it
        </saml:Audience>
      </saml:AudienceRestriction></saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-01-29T10:01:02Z">
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>
          urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1
        </saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance">
      <saml:Attribute Name="familyName">
        <saml:AttributeValue xsi:type="xsi:string">Rossi</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="spidCode">
        <saml:AttributeValue xsi:type="xsi:string">
          ABCDEFGHILMNOPQ
        </saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>

```

Listato 1 - Asserzione di autenticazione



Il protocollo *AuthnRequest* previsto per l'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

### 1.2.2.1. AUTHNREQUEST

L'*authnrequest* deve avere le seguenti caratteristiche:

- nell'elemento **<AuthnRequest>** devono essere presenti i seguenti attributi:
  - l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione *origine + timestamp* (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
  - l'attributo **IssueInstant** a indicare l'istante di emissione della richiesta, in formato UTC (esempio: "2008-03-13T18:04:15.531Z");
  - l'attributo **Destination**, a indicare l'indirizzo (URI reference) dell'*Identity provider* a cui è inviata la richiesta, come risultante nell'attributo **entityID** presente nel metadata IdP dell'*Identity Provider* a cui viene inviata la richiesta;
  - l'attributo **ForceAuthn** nel caso in cui si richieda livelli di autenticazione superiori a *SPIDL1* (*SPIDL2* o *SPIDL3*);
  - l'attributo **AssertionConsumerServiceIndex**, riportante un indice posizionale facente riferimento ad uno degli elementi **<AttributeConsumingService>** presenti nei *metadata* del *Service Provider*, atto ad indicare, mediante l'attributo **Location**, l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione, e mediante l'attributo **Binding**, il *binding* da utilizzare, quest'ultimo valorizzato obbligatoriamente con "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST";
  - in alternativa al precedente attributo (scelta sconsigliata) possono essere presenti
    - l'attributo **AssertionConsumerServiceURL** ad indicare l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione (l'indirizzo deve coincidere con quello del servizio riportato dall'elemento **<AssertionConsumingService>** presente nei *metadata* del *Service Provider*);
    - l'attributo **ProtocolBinding**, identificante il binding da utilizzare per inoltrare il messaggio di risposta, valorizzato con "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST";
- nell'elemento **<AuthnRequest>** può essere opzionalmente l'attributo:
  - **AttributeConsumingServiceIndex** riportante un indice posizionale in riferimento alla struttura **<AttributeConsumingService>** presente nei *metadata* del *Service*



*Provider*, atta a specificare gli attributi che devono essere presenti nell'asserzione prodotta. Nel caso l'attributo fosse assente l'asserzione prodotta non riporterà alcuna attestazione di attributo;

- può essere presente l'elemento **<Subject>** a indicare il soggetto per cui si chiede l'autenticazione in cui deve comparire:
  - l'elemento **<NameID>** atto a qualificare il soggetto in cui sono presenti i seguenti attributi:
    - **Format** che deve assumere il valore “*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*” (cfr. SAMLCore, sez. 8.3);
    - **NameQualifier** che qualifica il dominio a cui afferisce tale valore (URI);
- nell' elemento **<AuthnRequest>** non deve essere presente l'attributo **IsPassive** ( ad indicare “false” come valore di default);
- deve essere presente l'elemento **<Issuer>** aggiornato come l'attributo **entityID** riportato nel corrispondente SP *metadata*, a indicare l'identificatore univoco del *Service Provider* emittente. L'elemento deve riportare gli attributi:
  - **Format** fissato al valore “*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*”;
  - **NameQualifier** che qualifica il dominio a cui afferisce tale valore (URI riconducibile al *Service Provider* stesso);
- deve essere presente l'elemento **<NameIDPolicy>** avente il relativo attributo **AllowCreate**, se presente, valorizzato a “true” e l'attributo **Format** valorizzato come “*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*”;
- l'elemento **<Conditions>** se presente deve indicare i limiti di validità attesi dell'asserzione ricevuta in risposta, per esempio specificando gli attributi **NotBefore** e **NotOnOrAfter** opportunamente valorizzati in formato UTC;

**N.B. L'Identity Provider non è obbligato a tener conto dell'indicazione nel caso che questa non sia confacente con i criteri di sicurezza da esso adottati.**

- deve essere presente l'elemento **<RequestedAuthnContext>** (cfr. [SAMLCore], sez. 3.3.2.2.1) ad indicare il contesto di autenticazione atteso, ossia la “robustezza” delle credenziali richieste. Allo scopo sono definite le seguenti “*authentication context class*” estese (cfr.[SAMLAuthContext] sez. 3) in riferimento SPID:
  - *urn:oasis:names:tc:SAML:2.0:ac:classes: SpidL1*
  - *urn:oasis:names:tc:SAML:2.0:ac:classes: SpidL2*
  - *urn:oasis:names:tc:SAML:2.0:ac:classes: SpidL3*

referenziate dagli elementi **<AuthnContextClassRef>**. Ciascuna di queste classi, indica in ordine di preferenza il contesto di autenticazione (atteso o effettivo) secondo alcune dimensioni di riferimento, quali per esempio i meccanismi di autenticazione con cui l'*Identity*



*Provider* può identificare l'utente. L'elemento **<RequestedAuthnContext>** prevede un attributo **Comparison** con il quale indicare il metodo per stabilire il rispetto del vincolo sul contesto di abilitazione: i valori ammessi per questo attributo sono “*exact*”, “*minimum*”, “*better*”, “*maximum*”. Nel caso dell'elemento **<RequestedAuthnContext>**, questa informazione si riflette sulle tipologie di meccanismi utilizzabili dall'*Identity Provider* ai fini dell'autenticazione dell'utente. L'esempio di **<RequestedAuthnContext>** riportato nel Listato 2 - RequestedAuthnContext fa riferimento a una “*authentication context class*” di tipo “*SpidL2*” o superiore.

```
<samlp:RequestedAuthnContext Comparison="minimum">
  <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
  </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

Listato 2 - RequestedAuthnContext

**N.B.** L'*Identity Provider* ha facoltà di utilizzare per l'autenticazione un livello SPID più alto rispetto a quelli risultanti dall'indicazione del richiedente mediante l'attributo **Comparison**. Tale scelta non deve comportare un esito negativo della richiesta.

- nel caso del binding HTTP POST deve essere presente l'elemento **<Signature>** contenente la firma sulla richiesta apposta dal *Service Provider*. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- se presente l'elemento **<Scoping>** il relativo attributo **ProxyCount** deve assumere valore “0” per indicare che l'*Identity Provider* invocato non può delegare il processo di autenticazione ad altra *Asserting Party*;
- eventuali elementi **<RequesterID>** contenuti devono indicare l'URL del servizio di reperimento metadati di ciascuna delle entità che hanno emesso originariamente la richiesta di autenticazione e di quelle che in seguito la hanno propagata, mantenendo l'ordine che indichi la sequenza di propagazione (il primo elemento **<RequesterID>** dell'elemento **<Scoping>** è relativo all'ultima entità che ha propagato la richiesta);

Gli elementi **<Scoping>** **<RequesterID>** sono previsti per futuri usi ed al momento non devono essere utilizzati.



```

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_4d38c302617b5bf98951e65b4cf304711e2166df20"
  Version="2.0"
  IssueInstant="2015-01-29T10:00:31Z"
  Destination="https:// spidldp.spidldpProvider.it "
  AssertionConsumerServiceURL="http://spidSp.spidSpProvider.it"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AttributeConsumingServiceIndex="1">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
  <saml:Issuer
    NameQualifier=" http://spid-sp.it"
    Format=" urn:oasis:names:tc:SAML:2.0:nameid-format:entity " >
    SPID-sp-test
  </saml:Issuer>
  <samlp:NameIDPolicy
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
  <samlp:RequestedAuthnContext
    Comparison="exact">
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>

```

Listato 3 - AuthnRequest

#### 1.2.2.2. RESPONSE

Le caratteristiche che deve avere la risposta inviata dall'*Identity Provider* al *Service Provider* a seguito di una richiesta di autenticazione sono le seguenti:

- nell' elemento **<Response>** devono essere presenti i seguenti attributi:
  - l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) (cfr. UUID) o su una combinazione *origine + timestamp* ( quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - deve essere presente l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
  - deve essere presente l'attributo **IssueInstant** a indicare l'istante di emissione della risposta, in formato UTC;



- deve essere presente l'attributo ***InResponseTo***, il cui valore deve fare riferimento all'ID della richiesta a cui si risponde;
- deve essere presente l'attributo ***Destination***, a indicare l'indirizzo (URI reference) del *Service provider* a cui è inviata la risposta;
- deve essere presente l'elemento **<Status>** a indicare l'esito della AuthnRequest secondo quanto definito nelle specifiche SAML (cfr. [SAML-Core] par. 3.2.2.1 e ss.) comprendente il sotto-elemento **<StatusCode>** ed opzionalmente i sotto-elementi **<StatusMessage>** **<StatusDetail>** (cfr [SPID-TabErr]);
- deve essere presente l'elemento **<Issuer>** a indicare l'*entityID* dell'entità emittente, cioè l'*Identity Provider* stesso; L'attributo format deve essere omesso o assumere valore "urn:oasis:names:tc:SAML:2.0:nameid-format:entity";
- deve essere presente un elemento **<Assertion>** ad attestare l'avvenuta autenticazione, contenente almeno un elemento **<AuthnStatement>**; nel caso l'*Identity Provider* abbia riscontrato un errore nella gestione della richiesta di autenticazione l'elemento **<Assertion>** non deve essere presente;
- può essere presente l'elemento **<Signature>** contenente la firma sulla risposta apposta dall'*Identity Provider*. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

Per l'asserzione veicolata resta valido quanto già specificato nel paragrafo 1.2.1.



```

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_66bc42b27638a8641536e534ec09727a8aaa"
  Version="2.0"
  InResponseTo="_4d38c302617b5bf98951e65b4cf304711e2166df20"
  IssueInstant="2015-01-29T10:01:03Z"
  Destination="http://spid-sp.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
  <saml:Issuer
    NameQualifier="https://spidIdp.spidIdpProvider.it"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    spididp.it
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    .....
  </ds:Signature>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
      .....
    </saml:Assertion>
  </samlp:Response>

```

Listato 4 - Response (AuthnRequest)

## 1.2.2. CARATTERISTICHE DEL BINDING

### 1.2.2.1. BINDING HTTP REDIRECT

Nel caso del binding HTTP Redirect la richiesta viene veicolata con le seguenti modalità:

- come risposta alla richiesta di accesso dell'*end user* ad un servizio o risorsa, il *Service Provider* invia allo *User Agent* un messaggio HTTP di redirectione, cioè avente uno status code con valore 302 ("*Found*") o 303 ("*See Other*");
- il *Location Header* del messaggio HTTP contiene l'URI di destinazione del servizio di Single Sign-On esposto dall' *Identity Provider*. L'interfaccia è sempre la *IAuthnRequest*);
- il messaggio HTTP trasporta i seguenti parametri (tutti URL-encoded):
  1. "**SAMLRequest**": un costrutto SAML <**AuthnRequest**> codificato in formato *Base64* e compresso con algoritmo *DEFLATE*. Come da specifica, il messaggio SAML non contiene la firma in formato *XML Digital Signature* esteso (come avviene



in generale nel caso di binding HTTP POST). Ciò a causa delle dimensioni eccessive che esso raggiungerebbe per essere veicolato in una *query string*. La specifica indica come modalità alternativa quella di specificare con parametri aggiuntivi l'algoritmo utilizzato per firmare e la stringa con la codifica *Base64 URL-encoded* dei byte del messaggio SAML;

2. “**RelayState**”: identifica la risorsa (servizio) originariamente richiesta dall'utente e a cui trasferire il controllo alla fine del processo di autenticazione. Il *Service Provider* a tutela della privacy dell'utente nell'utilizzare questo parametro deve mettere in atto accorgimenti tali da rendere minima l'evidenza possibile sulla natura o tipologia della risorsa (servizio) richiesta;
3. “**SigAlg**”: identifica l'algoritmo usato per la firma prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore; il valore esteso di questo parametro è contestualizzato da un *namespace* appartenente allo standard *XML Digital Signature*. Come indicato al punto 1, tuttavia, la firma prodotta non fa uso della struttura XML definita in tale standard;
4. “**Signature**”: contiene la firma digitale della *query string*, così come prodotta prima di aggiungere questo parametro, utilizzando l'algoritmo indicato al parametro precedente;
5. Il browser dell'utente elabora quindi tale messaggio *HTTP Redirect* indirizzando una richiesta HTTP con metodo GET al servizio di Single Sign-On dell' *Identity Provider* (interfaccia *IAuthnRequest*) sotto forma di URL con tutti i sopraindicati parametri contenuti nella *query string*.

Un esempio di tale URL è il seguente, nel quale sono evidenziati in grassetto i parametri citati (i valori di alcuni parametri sono stati ridotti per brevità, inoltre il valore del parametro “**RelayState**” è stato reso non immediatamente intellegibile, come suggerito dalla specifica, sostituendo la stringa in chiaro con l'Id della richiesta: il *Service Provider* tiene traccia della corrispondenza):

```
https://idp.cnipa.gov.it:6443/idp/SSOServiceProxy?
SAMLRequest=nVPLbtswELz3KwTeZb0M2SYsBa6NoAbSRrGUHnqjqFVDQCJVLuU4f19KlhEDbVygR5K7O7Mzw%2
FXdqW2cI2gUSiYkmPnEAclVJtPhDwX9%2B6S3KWf1sJapqOb3rzIA%2FzqAY2zQQRtbNtWSe
[...]
ZwPAU88aUQvQ%2F8oe8S68piBDNabB5s3AyThb1XZMCxxEhhPj5qLZddW2sZICoP4fBW%2BWccqH0fz6iNir0tU
QGeCWZaGZxE5pM4n8Nz7p%2Be2D3S6L51x1N1jO%2BCO2qh8zO%2Bji%2FfnN098%3D&RelayState=s29f6c7d
6bbf9e62968d27309e2e4beb6133663a2e&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig
%23rsa-sha1&Signature=LtNj%2BbMc8j%2FhglWzHPMmo0ESQzBaWlmQbZxas%2B%2FI fNO4F%2F7WNOMKDZ4
VVEBtCEQKWp12pU7vPB5WVVMRMrGB8ZRadHmPp0hJ9opO3NdafRc04Z%2BbfnkSuQCN9NcGV%2BajT
[...]
ra169jhaGRReRQ9KkgSB3aTpQGaffAYUPVo2XZiWy6f9Z7zsmV%2FFoT8dg%3D%3D
```

Listato 5 - http redirect query string

### 1.2.2.2. BINDING HTTP POST

Nel caso del *binding* HTTP POST, come risposta alla richiesta di accesso dell'utente ad un



servizio o risorsa, il SP invia allo *User Agent* (il browser dell'utente) un messaggio HTTP con status code avente valore 200 ("OK"):

- il messaggio HTTP contiene una *form* HTML all'interno della quale è trasportato un costrutto SAML <**AuthnRequest**> codificato come valore di un *hidden form* control di nome "*SAMLRequest*". Rispetto al binding HTTP Redirect, l'utilizzo di una *form* HTML permette di superare i limiti di dimensione della *query string*. Pertanto, l'intero messaggio SAML in formato XML può essere firmato in accordo alla specifica *XML Digital Signature*. Il risultato a valle della firma è quindi codificato in formato *Base64*;
- la *form* HTML contiene un secondo *hidden form* control di nome "*RelayState*" che contiene il corrispondente valore del *Relay State*, cioè della risorsa originariamente richiesta dall'utente e alla quale dovrà essere trasferito il controllo al termine della fase di autenticazione;
- la *form* HTML è corredata da uno script che la rende auto-postante all'indirizzo indicato nell'attributo "*action*";
- Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST verso il componente *Single Sign-On* dell'*Identity Provider* (interfaccia *IAuthnRequest*).

Un esempio di *form* HTML per trasferire in HTTP POST la richiesta di autenticazione è descritto nel listato 1.4. Osservando attentamente il codice riportato in figura si può notare il valore del parametro "*SAMLRequest*" (ridotto per brevità); il valore del parametro *RelyState* reso non immediatamente intellegibile (cfr. sez. precedente); l'elemento <**input** type="submit" value="Go"/>, che ha lo scopo di visualizzare all'interno del web browser il pulsante di invio della form utilizzabile dall'utente, non strettamente necessario in quanto la *form* è resa auto-postante.

```
<html>
<body onload="javascript:document.forms[0].submit()">
<form method="post" action="https://lp.cnipa.gov.it:6443/lp/SSOServiceProxy">
<input type="hidden" name="RelayState"
      value="s2645f48777bd62ec83eddc62c066da5cb987c1eb3">
<input type="hidden" name="SAMLRequest"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluc2Z0iVVRGLTgiPz4KPHNhbnBwXwOkF1dGhuUmVxdWVzdCBBC3N1cnRpb25Db25zdW1lc1N1cnRpb25VUkw9Imh0dHA6Ly9zcC5pY2FyLml00jgwODAvAaWNhc
[...]
```

N0ZWRUcmFuc3BvcnQ8L3NhbnBw6QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1scDpSZXF1ZXN0ZWRBdXR0bkNvb  
nRleHQ+PHNhbnBwXw01NjB3BpbmcgUHJveH1Db3VudD0iMiIgeG1sbnM6c2FtbHA9InVyb2pYXNpczpuYW1lc2p0  
YzptQU1MOjIUMDpwcml0b2NvbCIvPjwvc2FtbHA6QXV0aG5SZXF1ZXN0Pg== ">

```
<input type="submit" value="Go"/>
</form>
</body>
</html>
```

Listato 6 - Richiesta http POST bindig

Conclusa la fase di autenticazione, l'*Identity Provider* costruisce una <**Response**> firmata diretta al *Service Provider*, e in particolare al relativo servizio *AssertionConsumerService*. La <**Response**> viene inserita in una *form* HTML come campo nascosto di nome "*SAMLResponse*". L'*Identity Provider* invia la *form* HTML al browser dell'utente in una risposta HTTP.



Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST contenente la **<Response>** firmata verso il *Service Provider*.

Un esempio di tale *form* è riportato nel listato 1.8 (anche in questo caso, il valore del parametro "**SAMLResponse**" è stato ridotto per brevità).

```
<html>
<body onload="javascript:document.forms[0].submit()">
<form method="post"
action="http://rp.cnipa.gov.it:8080/cniparp/AssertionConsumerService">
<input type="hidden" name="SAMLResponse"
value="PD94bWwgdmVyc2lvcj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbwXwOlJlc3BvbnNlIERlc3Rp
bmF0aW9uPSJodHRwOi8vc3AuaWNhcn5pdDo4MDgwL2l jYXItc3AvQXNzZXJ0aW9uQ29uc3VtZXJtZXJ2aWNlIiB
JRD0ic3JhNTdmN2RhYTUyMTc2NWZmOTQ2ODM0ZmY2NjIzNTA3ZTcwNGI1MDQ3IiBJblJlc3BvbnNlVG89InMyOG
Q5MWEyNmJkNGQ2MGY0N2E0OTkxMzMwMGZhZjc2MzFiZjMxNDBlOSIgSXNzdWVJbnN0YW50PSIyMDA4LTAzLTA0V
DIyOjEzOjQ4LjUwMFoiIFZlcnNpb249IjIuMCIgeG1sbnM6c2Ftb
[... ]
21zOm5hbWVzOnRjOlNBTUw6Mi4wOmFjOmNsYXNzZXM6UGFzc3dvcnRQcm90ZWN0ZWRUcmFuc3BvcnQ8L3Nhbw6
QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1sOkF1dGhuQ29udGV4dD48L3Nhbw6QXV0aG5TdGF0ZW11bnQ+PC9
zYW1sOkFzc2VydGlvbj48L3NhbwXwOlJlc3BvbnNlPg==">
<input type="hidden" name="RelayState"
value="s28d91a26bd4d60f47a49913300faf7631bf3140e9">
<input type="submit" value="Go"/>
</form>
</body>
</html>
```

Listato 7 - Risposta http POST binding

### 1.2.2.3. GESTIONE DELLA SICUREZZA SUL CANALE DI TRASMISSIONE

Il profilo SAML SSO raccomanda l'uso di SSLv.3.0 o TLS 1.0 nei colloqui tra *Asserting party* (*Identity Provider* e *Attribute Authority*), le *Relying Party* (*Service Provider*) e lo *user agent*. In ambito SPID si rende obbligatorio l'impiego di TLS nella versione più recente disponibile.

### 1.2.2.4. IDP METADATA

Le caratteristiche dell'*Identity provider* devono essere definite attraverso *metadata* conformi allo standard SAMLv2.0. (cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

- nell'elemento **<EntityDescriptor>** devono essere presenti i seguenti attributi:
  - **entityID**: indicante l'identificativo (URI); dell'entità univoco in ambito SPID;
- l'elemento **<IDPSSODescriptor>** specifico che contraddistingue l'entità di tipo *Identity provider* deve riportare i seguenti attributi:
  - **protocolSupportEnumeration**: che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "*urn:oasis:names:tc:SAML:2.0:protocol*");
  - **WantAuthnRequestSigned**: attributo con valore booleano che impone ai service provider che fanno uso di questo Identity provider l'obbligo della firma delle richieste di autenticazione;

al suo interno devono essere presenti:



- l'elemento **<KeyDescriptor>** che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (cfr.[SAML-Metadata], sez. 2.4.1.1);
- l'elemento **<KeyDescriptor>** che contiene il certificato della corrispondente chiave pubblica dell'entità, utile per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (cfr.[SAML-Metadata], sez. 2.4.1.1);
- l'elemento **<NameIDFormat>** riportante l'attributo:
  - **format**, indicante il formato "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*" come quello supportato per l'elemento di **<NameID>** utilizzato nelle richieste e risposte SAML per identificare il *subject* cui si riferisce un'asserzione;
- uno o più elementi **<SingleSignOnService>** che specificano l'indirizzo del Single Sign-On Service riportanti i seguenti attributi:
  - **Location** url endpoint del servizio per la ricezione delle richieste;
  - **Binding** che può assumere uno dei valori:
    - "*urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect*"
    - "*urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST*";

opzionalmente possono essere presenti:

- uno o più elementi **<attribute>** ad indicare nome e formato degli attributi certificabili dell'Identity provider (cfr. Tabella attributi SPID), riportanti gli attributi:
  - **Name** nome dell'attributo ( colonna *identificatore* della Tabella attributi SPID);
  - **xsi:type** tipo dell'attributo ( colonna *tipo* della Tabella attributi SPID);
- deve essere l'elemento **<Signature>** riportante la firma sui *metadata* . La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- è consigliata la presenza di un elemento **<Organization>** a indicare l'organizzazione a cui afferisce l'entità specificata, riportante gli elementi:
  - **<OrganizationName>** indicante un identificatore *language-qualified* dell'organizzazione a cui l'entità afferisce;
  - **<OrganizationURL>** \ riportante in modalità *language-qualified* la url istituzionale dell'organizzazione.



```

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
  entityID="http://spidIdp.idpProvider.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
  <md:IDPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> .....</md:KeyDescriptor>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </md:NameIDFormat>
    <md:SingleSignOnService
      Location="https://spidIdp.idpProvider.it/redirect-Post-saml2sso"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <md:SingleSignOnService
      Location="https://spidIdp.idpProvider.it/Post-Post-saml2sso"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <saml:Attribute xsi:type="xsi:string" Name="familyName"/>
    <saml:Attribute xsi:type="xsi:string" Name="name"/>
    <saml:Attribute xsi:type="xsi:string" Name="spidCode"/>
    <saml:Attribute xsi:type="xsi:string" Name="fiscalNumber"/>
    <saml:Attribute xsi:type="xsi:string" Name="gender"/>
    <saml:Attribute xsi:type="xsi:string" Name="dateOfBirth"/>
    <saml:Attribute xsi:type="xsi:string" Name="placeOfBirth"/>
    <saml:Attribute xsi:type="xsi:string" Name="companyName"/>
    <saml:Attribute xsi:type="xsi:string" Name="registeredOffice"/>
    <saml:Attribute xsi:type="xsi:string" Name="ivaCode"/>
    <saml:Attribute xsi:type="xsi:string" Name="idCard"/>
    <saml:Attribute xsi:type="xsi:string" Name="mobilePhone"/>
    <saml:Attribute xsi:type="xsi:string" Name="email"/>
    <saml:Attribute xsi:type="xsi:string" Name="address"/>
    <saml:Attribute xsi:type="xsi:string" Name="digitalAddress"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

#### Listato 8 - Metadata IdP

I *metadata Identity Provider* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL `<dominioGestoreIdentita>/metadata`, ove non diversamente specificato *nel Registro SPID*, e saranno firmate dell'*Agenzia per l'Italia Digitale*. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.





### 1.3. FORNITORE DEI SERVIZI

Il *fornitore di servizi* denominato anche con il termine tecnico di *Service Provider* per la realizzazione dei profili SSO previsti, *SP-Initiated* Redirect/POST binding e POST/POST binding, deve mettere a disposizione le seguenti interfacce:

- **IAuthnResponse**: ricezione delle risposte di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei SAML metadata del *Service Provider* da parte dell'*Identity Provider*.

#### 1.3.1. REGOLE DI PROCESSAMENTO DELLA <RESPONSE>

Alla ricezione <**response**> qualunque sia il *binding* utilizzato il *Service Provider* prima di utilizzare l'asserzione deve operare almeno le seguenti verifiche:

- controllo delle firme presenti nella <**Assertion**> e nella <**response**>;
- nell'elemento <**SubjectConfirmationData**> verificare che:
  - l'attributo **Recipient** coincida con la assertion consuming service URL a cui la <**Response**> è pervenuta;
  - l'attributo **NotOnOrAfter** non sia scaduto;
  - l'attributo **InResponseTo** riferisca correttamente all'ID della <**AuthnRequest**> di richiesta.

Il fornitore di servizi deve garantire che le asserzioni non vengano ripresentate, mantenendo il set di identificatori di richiesta (**ID**) usati come per le <**AuthnRequest**> per tutta la durata di tempo per cui l'asserzione risulta esser valida in base dell'attributo **NotOnOrAfter** dell'elemento <**SubjectConfirmationData**> presente nell'asserzione stessa.

#### 1.3.2. SP METADATA

Le caratteristiche del *Service Provider* devono essere definite attraverso metadata conformi allo standard SAMLv2.0. (cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

- nell'elemento <**EntityDescriptor**> devono essere presenti i seguenti attributi:
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
- deve l'elemento <**KeyDescriptor**> contenere il certificato della corrispondente chiave pubblica dell'entità, utile per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (cfr. [SAML-Metadata], sez. 2.4.1.1);
- deve essere l'elemento <**Signature**> riportante la firma sui *metadata*. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;



- deve essere presente l'elemento **<SPSSODescriptor>** riportante i seguenti attributi:
  - **protocolSupportEnumeration**: che enumera, separati da uno spazio, gli URI associati ai protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "**urn:oasis:names:tc:SAML:2.0:protocol**");
  - **AuthnRequestSigned**: valorizzato *true* attributo con valore booleano che esprime il requisito che le richieste di autenticazione inviate dal service provider siano firmate;
- deve essere presente almeno un elemento **<AssertionConsumerService>** indicante il servizio (in termini di URL e relativo binding "HTTP POST") a cui contattare il *Service Provider* per l'invio di risposte SAML, riportanti i seguenti attributi:
  - **index** che può assumere valori unsigned;
  - **Binding** posto al valore "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST**";
  - **Location** url endpoint del servizio per la ricezione delle risposte;

In particolare il primo di questi elementi (o l'unico elemento riportato) deve obbligatoriamente riportare:

- l'attributo **index** posto al valore 0;
  - l'attributo **isDefault** posto al valore *true*;
- deve essere presente uno o più elementi **<AttributeConsumingService>** a descrizione dei set di attributi richiesti dal *Service Provider*, riportante:
    - l'attributo **index**, indice posizionale dell'elemento relativo all'i-esimo servizio richiamato dalla authReq mediante l'attributo **AttributeConsumingServiceIndex** dell'elemento **<AuthnRequest>**;
    - l'elemento **<ServiceName>**, riportante l'identificatore dell'i-esimo set minimo di attributi necessari<sup>1</sup> per l'autorizzazione all'accesso;
    - uno o più elementi di tipo **<RequestedAttribute>**, ciascuno di essi costituente la lista degli attributi associati all'i-esimo servizio;
  - è consigliata la presenza di un elemento **<Organization>** a indicare l'organizzazione a cui afferisce l'entità specificata, riportante gli elementi:
    - **<OrganizationName>** indicante un identificatore *language-qualified* dell'organizzazione a cui l'entità afferisce;
    - **<OrganizationURL>** riportante in modalità *language-qualified* la url istituzionale dell'organizzazione.

<sup>1</sup> Per la massima tutela della privacy dell'utente il *service provider* deve rendere minima la visibilità dei servizi effettivamente invocati. In questa logica occorre rendere ove possibile indifferenziate le richieste relative a servizi che condividono lo stesso set minimo di attributi necessari per l'autorizzazione.





I *metadata Services Provider* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL `< dominioServiceProvider >/metadata` e saranno firmate dell' *Agenzia per l'Italia Digitale*. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

#### 1.4. ELENCO DEGLI ATTRIBUTI E MESSAGGI DI ERRORE

L'elenco degli attributi certificabili ed i messaggi di anomalia relativi agli scambi SAML sono descritti nelle relative tabelle pubblicate presso il sito dell' *Agenzia per l'Italia Digitale*.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https:// spidSP.serviceProvider.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
  <md:SPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    AuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> ..... </md:KeyDescriptor>
    <md:AssertionConsumerService
      index="0"
      Location="https:// spidSP.serviceProvider.it /Location_0"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:AssertionConsumerService
      index="1"
      Location="https:// spidSP.serviceProvider.it /Location_1"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:AttributeConsumingService index="0">
      <md:ServiceName xml:lang="it">set0</md:ServiceName>
      <md:RequestedAttribute Name="name"/>
      <md:RequestedAttribute Name="familyName"/>
      <md:RequestedAttribute Name="fiscalNumber"/>
      <md:RequestedAttribute Name="email"/>
    </md:AttributeConsumingService>
    <md:AttributeConsumingService index="1">
      <md:ServiceName xml:lang="it" >set1</md:ServiceName>
      <md:RequestedAttribute Name="name"/>
      <md:RequestedAttribute Name="familyName"/>
      <md:RequestedAttribute Name="fiscalNumber"/>
      <md:RequestedAttribute Name="email"/>
    </md:AttributeConsumingService>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Listato 9 - Metadata SP



## 2 REGOLE TECNICHE PER IL GESTORE DI ATTRIBUTI QUALIFICATI

Un *Gestore di attributi qualificati*, nel seguito indicato anche con il termine tecnico *Attribute Authority*, deve essere in grado di certificare un determinato set di attributi relativi ad un soggetto titolare di una identità digitale. A fronte di una richiesta di uno o più attributi l'*Attribute Authority* deve essere in grado di:

1. ricevere ed interpretare la richiesta di attributo pervenuta da una *Service Provider*;
2. elaborare la richiesta;
3. costruire la risposta inerente la richiesta pervenuta ed inoltrarla alla *Service Provider*.

Il componente *Attribute Authority* deve esporre le seguenti interfacce:

- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di richiesta di attributo SAML;
- **IMetadataRetrive**: permette il reperimento dei *SAML metadata* da parte delle *Service Provider*.

### 2.1. SCENARIO DI INTERAZIONE

	Descrizione	Interfaccia	SAML	Binding
1	La <i>Service Provider</i> invia all' <i>Attribute Authority</i> una richiesta di attributi. Ciò avviene utilizzando il costrutto <b>&lt;AttributeQuery&gt;</b> della specifica SAML e interagendo mediante "SAML SOAP binding".	IAttributeQuery	<AttributeQuery>	SOAP Over HTTP
2	L' <i>Authority Registry</i> elabora la richiesta ricevuta.	-	-	-
3	La <i>Attribute Authority</i> risponde alla richiesta di attributi del <i>Service Provider</i> con una <b>&lt;Response&gt;</b> SAML contenente l'asserzione, interagendo mediante "SAML SOAP binding".	IAttributeQuery	<Response>	SOAP Over HTTP

Tabella 2 - AttributeRequest



## 2.2. SPECIFICHE DELLE INTERFACCE

Di seguito vengono espone le specifiche delle interfacce dell'*Attribute Authority* riportanti:

- le caratteristiche delle asserzioni prodotte;
- le caratteristiche delle *AttributeQuery* e della *Response*;
- le caratteristiche del *binding*;
- i metadati.

### 2.2.1. CARATTERISTICHE DELLE ASSEZIONI

Le asserzioni prodotte dall'*Attribute Authority* devono essere conformi allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

L'*Asserzione* deve avere le seguenti caratteristiche:

- nell'elemento **<Assertion>** devono essere presenti i seguenti attributi:
  - l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
  - l'attributo **IssueInstant** a indicare l'istante di emissione della richiesta, in formato UTC (esempio: "2008-03-13T18:04:15.531Z");
- deve essere presente l'elemento **<Subject>** a indicare il soggetto a cui si riferiscono gli attributi in cui deve comparire:
  - l'elemento **<NameID>** atto a qualificare il soggetto dell'asserzione, in cui sono presenti i seguenti attributi:
    - **Format** che deve assumere il valore "*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*" (cfr. SAMLCore, sez. 8.3);
    - **NameQualifier** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Attribute Authority*);
- l'elemento **<Issuer>** a indicare l'*entityID* dell'*Attribute Authority* emittente ( attualizzato come l'attributo **entityID** presente nei corrispondenti AAA *metadata*.) con l'attributo **Format** riportante il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";
- deve essere presente l'elemento **<Conditions>** in cui devono essere presenti gli attributi:
  - **NotBefore**,
  - **NotOnOrAfter**;



e l'elemento:

- **<AudienceRestriction>** riportante a sua volta l'elemento **<Audience>** attualizzato con l'*entityID* del *ServiceProvider* per il quale l'asserzione è emessa;
- deve essere presente l'elemento **<AttributeStatement>** riportante gli attributi certificati dall'*Attribute Authority*. Tale elemento dovrà comprendere uno o più elementi di tipo **<Attribute>**;
- un elemento di tipo **<Attribute>** relativo ad un attributo certificato dovrà comprendere:
  - l'attributo **Name** attualizzato con identificativi di attributo definiti nella tabella attributi SPID (cfr. SPID - Tabella attributi);
  - uno o più elementi **<AttributeValue>** ciascuno riportante l'attributo **Type** (cfr. SPID - Tabella attributi) e attualizzato con il valore assunto dall'attributo;
- l'elemento **<Assertion>** può eventualmente presentare l'elemento **<Advice>**, contenente altri elementi **<Assertion>** di cui è necessario fornire evidenza in forma originale in sede di risposta alla richiesta di attributo;
- l'elemento **<Signature>** riportante la firma sull'asserzione apposta dall'*Identity Provider* emittente. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

```

<ns2:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_27e00421b56a5aa5b73329240ce3bb832caa"
  IssueInstant="2015-01-29T10:01:03Z"
  Version="2.0" >
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
  <ns2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    spidIAA.spidiAADomain.it
  </ns2:Issuer>
  <ns2:Subject>
    <ns2:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
      NameQualifier="http://spidIAA.spidiAADomain.it">
        TINIT-BNLFNC68E28F205T
    </ns2:NameID>
  </ns2:Subject>
  <saml:Conditions NotBefore="2015-01-29T10:00:33Z" NotOnOrAfter="2015-01-29T10:02:33Z" >
    <saml:AudienceRestriction>
      <saml:Audience>
        https:// spidSP.serviceProvider.it
      </saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <ns2:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance" >
    <ns2:Attribute Name="NomeAttributo">
      <ns2:AttributeValue xsi:type="xsi:string">ValoreAttributo</ns2:AttributeValue>
    </ns2:Attribute>
  </ns2:AttributeStatement>
</ns2:Assertion>

```

Listato 10- Asserzione di attributo

### 2.2.2. CARATTERISTICHE DELLE ATTRIBUTEQUERY E DELLA RESPONSE

Il protocollo *attributeQuery* previsto per l'*Attribute Authority* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

#### 2.2.2.1. ATTRIBUTEQUERY

L' *attributeQuery* deve avere le seguenti caratteristiche:

- nell' elemento **<AttributeQuery>** devono essere presenti i seguenti attributi:
  - l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione *origine + timestamp*;
  - l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione



della specifica SAML adottata;

- l'attributo **IssueInstant** a indicare l'istante di emissione della richiesta, in formato UTC;
- l'attributo **Destination**, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService della *Attribute Authority*;
- deve essere presente l'elemento <**Issuer**> a indicare l'identificatore univoco del *Service Provider* emittente aggiornato come l'attributo **entityID** riportato nel corrispondente *SP metadata*. L'elemento deve riportare l'attributo **Format** aggiornato con il valore "urn:oasis:names:tc:SAML:2.0:nameid-format:entity";
- deve essere presente l'elemento <**Subject**> a referenziare il soggetto a cui si riferisce la richiesta di attributo, in cui deve comparire:
  - l'elemento <**NameID**> aggiornato con il codice fiscale del soggetto (cfr. Tabella attributi SPID), in cui deve essere presente l'attributo:
    - **Format** che deve assumere il "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" (cfr. SAMLCore, sez. 8.3);
    - **NameQualifier** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Attribute Authority*);
- deve essere presente uno o più elementi <**Attribute**>, il cui attributo **Name** indica lo specifico attributo di cui si vuole conoscere il valore (cfr. SPID - Tabella attributi);
- in ciascun elemento <**Attribute**> possono essere presenti uno o più elementi <**AttributeValue**> per richiedere la verifica che l'attributo abbia i valori specificati;
- deve essere presente l'elemento <**Signature**> riportante la firma sull'asserzione apposta dall'*Identity Provider* emittente. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.



```

<samlp:AttributeQuery xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_4d38c302617b5bf98951e65b4cf304711e2166df20"
  Version="2.0"
  IssueInstant="2015-01-29T10:00:31Z"
  Destination="spidIAA.spidiAADomain.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://spidSP.spidSPDomain.it
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      NameQualifier="http://spidIAA.spidiAADomain.it"
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
      TNIT-BNLFNC68E28F205T
    </saml:NameID>
  </saml:Subject>
  <saml:Attribute
    Name="NomeAttributo"/>
</samlp:AttributeQuery>

```

Listato 11 - AttributeQuery

#### 2.2.2.2. RESPONSE

Le caratteristiche che deve avere la risposta inviata dall' *Attribute Authority* al *Service Provider* a seguito di una richiesta di attributi sono le seguenti:

- nell' elemento **<Response>** devono essere presenti i seguenti attributi:
  - deve essere presente l'attributo **ID** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) (cfr. UUID) o su una combinazione *origine + timestamp*;
  - deve essere presente l'attributo **Version**, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
  - deve essere presente l'attributo **IssueInstant** a indicare l'istante di emissione della risposta, in formato UTC;
  - deve essere presente l'attributo **InResponseTo**, il cui valore deve fare riferimento all'ID della richiesta a cui si risponde;
  - deve essere presente l'attributo **Destination**, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService del Service Provider;
- deve essere presente l'elemento **<Issuer>** a indicare l'identificatore univoco dall' *Attribute Authority* emittente aggiornato come l'attributo **entityID** riportato nel corrispondente *AA metadata*.. L'elemento deve riportare l'attributo **Format** aggiornato



con il valore “urn:oasis:names:tc:SAML:2.0:nameid-format:entity”;

- deve essere presente l'elemento **<Status>** a indicare l'esito della *attributeQuery* secondo quanto definito nelle specifiche SAML (cfr. [SAML-Core] par. 3.2.2.1 e ss.) comprendente il sotto-elemento **<StatusCode>** ed opzionalmente i sotto-elementi **<StatusMessage>** **<StatusDetail>** (cfr [SPID-TabErr]);
- deve essere presente l'elemento **<Assertion>** come specificato al paragrafo 2.3.1, contenenti elementi **<AttributeStatement>** relativi agli attributi richiesti;
- può presentare l'elemento **<Signature>** riportante la firma sull'asserzione apposta dall'*Identity Provider* emittente. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_66bc42b27638a8641536e534ec09727a8aaa"
  Version="2.0"
  InResponseTo="_4d38c302617b5bf98951e65b4cf304711e2166df20"
  IssueInstant="2015-01-29T10:01:03Z"
  Destination="http://spidIAA.spidiAADomain.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://spidAA.spidiAADomain.it
  </saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
      .....
    </saml:Assertion>
  </samlp:Response>
```

Listato 12 - Response (AuthnRequest)

### 2.2.3. CARATTERISTICHE DEL BINDING

Il binding previsto per il trasporto di messaggi è il SAML SOAPbinding su http(cfr. [SAML-Bin] par. 3.2.).





#### 2.2.4. ATTRIBUTE AUTHORITY METADATA

Le caratteristiche dell'*Attribute Authority* devono essere definite attraverso *metadata* conformi allo standard SAMLv2.0 (cfr. [SAML-Metadata]), e rispettare specificatamente le condizioni di seguito indicate:

- nell'elemento **<EntityDescriptor>** devono essere presenti i seguenti attributi:
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
- l'elemento **<AttributeAuthorityDescriptor>** specifico che contraddistingue l'entità di tipo *Attribute Authority*; deve riportare il seguente attributo:
  - **protocolSupportEnumeration**: che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "urn:oasis:names:tc:SAML:2.0:protocol");

inoltre al suo interno devono essere presenti:

- l'elemento **<KeyDescriptor>** che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (cfr.[SAML-Metadata], sez. 2.4.1.1);
- uno o più elementi **<AttributeService>** indicante il servizio a cui contattare l'*Attribute Authority* riportante i seguenti attributi:
  - **Binding** posto al valore "urn:oasis:names:tc:SAML:2.0:bindings:SOAP";
  - **Location** url endpoint del servizio per la ricezione delle richieste;
- l'elemento **<NameIDFormat>** riportante l'attributo:
  - **format**, indicante il formato "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" come quello supportato per l'elemento di **<NameID>** utilizzato nelle richieste e risposte SAML per identificare il *subject* cui si riferisce un'asserzione;
- **<AttributeProfile>**: enumerazione dei profili di rappresentazione di attributi supportati dall'entità (cfr.[SAML-Profile], sez. 8); nel caso specifico solo "basic" (cfr. [SAML-Profile], sez. 8.1);
- uno o più elementi **<Attribute>** riportanti gli attributi:
  - **Name** riportante l'identificativo dell'attributo;
  - **NameFormat** riportante il format dell'attributo;
- deve essere l'elemento **<Signature>** riportante la firma sui *metadata*. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- è consigliata la presenza di un elemento **<Organization>** a indicare l'organizzazione a cui afferisce l'entità specificata, riportante gli elementi:
  - **<OrganizationName>** indicante un identificatore *language-qualified*



- **<OrganizationURL>** dell'organizzazione a cui l'entità afferisce; importante in modalità language-qualified la url istituzionale dell'organizzazione.

I *metadata Attribute Authority* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL *<dominio.AttributiQualificati>/metadata*, ove non diversamente specificato *nel Registro SPID*, e saranno firmate dell'*Agenzia per l'Italia Digitale*. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
  entityID="https://spidAA.spidAASProvider.it">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
  <md:AttributeAuthorityDescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing"> .....</md:KeyDescriptor>
    <md:AttributeService
      Location="https://spidAA.spidAASProvider.it/AAService"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    <md:AttributeProfile>
      urn:oasis:names:tc:SAML:2.0:attrname-format:basic
    </md:AttributeProfile>
    <saml:Attribute Name="IdentificativoAttributo1"/>
    <saml:Attribute Name="IdentificativoAttributo2"/>
    <saml:Attribute Name="IdentificativoAttributo3"/>
  </md:AttributeAuthorityDescriptor>
</md:EntityDescriptor>
```

Listato 13 - Metadata AA

### 2.3. ELENCO DEGLI ATTRIBUTI E MESSAGGI DI ERRORE

L'elenco degli attributi certificabili ed i messaggi di anomalia relativi agli scambi SAML sono descritti nelle relative tabelle pubblicate presso il sito dell'*Agenzia per l'Italia Digitale*.



### 3 REGISTRO SPID

Il *Registro SPID* è il repository di tutte le informazioni relative alla entità aderenti a SPID e costituisce l'evidenza del cosiddetto *circle of trust* in esso stabilito.

La relazione di fiducia su cui si basa la federazione stabilita in SPID si realizza per il tramite dell'intermediazione dell'Agenzia, terza parte garante, attraverso il processo di accreditamento dei gestori dell'identità digitale, dei gestori degli attributi qualificati e dei fornitori di servizi. L'adesione a SPID costituisce l'instaurazione di una relazione di fiducia con tutti i soggetti già aderenti, accreditati dall'Agenzia, sulla base della condivisione dei livelli standard di sicurezza dichiarati e garantiti da SPID.

L'adesione al patto di fiducia tra le entità aderenti (gestori dell'identità digitale, gestori degli attributi qualificati e fornitori di servizi) si evidenzia nella presenza di tali entità nel *Registro SPID* gestito dall'Agenzia.

#### 3.1. CONTENUTI DEL REGISTRO

Il *federation registry* contiene la lista delle entità che hanno superato il processo di accreditamento e quindi facenti parte della federazione SPID. Le informazioni contenute nel registro per ciascuna delle suddette entità sono le seguenti:

- **AuthorityInfo** entry del registro relativa ad una entità; a sua volta costituita da:
  - **EntityId**: identificatore SAML dell'entità;
  - **Soggetto**: denominazione del soggetto a cui afferisce l'entità della federazione;
  - **EntityType**: tipo di entità (*Identity Provider, Attribute Authority, Service Provider*);
  - **MetadataProviderURL**: l'URL del servizio di reperimento metadati;
  - **AttributeList**: elenco di *attributi qualificati* certificabili da una entità di tipo *Attribute Authority*.

Il *federation registry* viene popolato dall'Agenzia per l'Italia Digitale a seguito del processo di stipula delle convenzioni e aggiornata dalla stessa Agenzia nel corso delle attività legate alla gestione delle convenzioni e della vigilanza sui soggetti del circuito SPID.

Il contenuto informativo della *federation registry* è in fruizione a tutte le entità appartenenti al circuito SPID ai fini della verifica della sussistenza di relazioni di trust nei confronti di entità terze (IdP, AA, SP) e del reperimento delle informazioni associate alle stesse. Il *Discovery Service* può anch'esso accedere al *federation registry* per utilizzarne i contenuti ai fini de attività di discovering.

##### 3.1.1. ACCESSO AL REGISTRO

L'accesso ai contenuti del *federation registry* avviene in modalità REST attraverso l'interfaccia (risorsa) **IRegistry**. In particolare:

- l'accesso in consultazione ai contenuti del directory avviene attraverso il metodo *http GET*



**request****parametri *query string*:**

- *entityId*:string per selezionare la entry relativa ad una determinata *entityId*; si usi \* come wildcard;
- *soggetto*:string per selezionare la entry relativa ad un determinato soggetto; si usi \* come wildcard;
- *authorityType*:string per selezionare le entry relative ad una determinata categoria di entità (IdP, AA); si usi \* come wildcard,
- *attributeType*:string per selezionare le entry relative ad entità in grado di certificare un determinato attributo qualificato; si usi \* come wildcard,

**response****status:** 200- OK*representation* application/xml

*formato risposta* secondo lo schema riportato nel  
 Listato 14 - federationRegistry.xsd      firmata *xml*  
*signature* [XMLSig].

**status:** 400 - Bad request**status:** 403 - Forbidden – User does not have privilege to read the resource**status** 404 - Not Found

Per l'accesso al registro si rende obbligatorio l'impiego di TLS nella versione più recente disponibile.

**3.1.1.1. ACCESSO AL REGISTRO IN MODALITA' LDAP**

Insieme o in alternativa alla modalità di accesso al *federation registry* precedentemente descritta potrà essere fornita una interfaccia di accesso interrogabile secondo il protocollo LDAP. Questa seconda modalità di accesso sarà relativa allo stesso contenuto informativo e funzionante secondo le stesse logiche di accesso descritti per l'interfaccia REST. Le specifiche di tale interfaccia saranno rese note in un separato documento pubblicato sul sito dell'Agenzia per l'Italia Digitale.



```

<SCHEMA xmlns="http://www.w3.org/2001/XMLSchema"

  xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://www.agid.gov.it/spid"
  xmlns:tns="http://www.agid.gov.it/spid" elementFormDefault="qualified">
    <import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="..." />
    <import namespace="http://www.w3.org/2001/04/xmlenc#" schemaLocation="..." />
    <element name="FederationRegistry" type="tns:FederationRegistryType"/>
    <complexType name="FederationRegistryType">
      <sequence>
        <element name="AuthorityInfo" type="tns:AuthorityInfoType"
          minOccurs="0" maxOccurs="unbounded"/>
      </sequence>
    </complexType>
    <complexType name="AuthorityInfoType">
      <sequence>
        <element name="EntityID" type="anyURI" maxOccurs="1" minOccurs="1"/>
        <element name="IdSoggetto" type="string" maxOccurs="1" minOccurs="1"/>
        <element name="EntityType" type="tns:entity" maxOccurs="1" minOccurs="1"/>
        <element name="MetadataProviderURL" type="anyURI" maxOccurs="1" minOccurs="1"/>
        <element name="AttributeList" type="tns:attributeListType" maxOccurs="1" minOccurs="0"/>
      </sequence>
    </complexType>
    <complexType name="attributeListType">
      <sequence>
        <element name="Attribute" type="tns:qualifiedAttributeType"
          minOccurs="1" maxOccurs="unbounded"/>
      </sequence>
    </complexType>
    <simpleType name="entity">
      <restriction base="xs:string">
        <enumeration value="IdP"/>
        <enumeration value="AA"/>
        <enumeration value="SP"/>
      </restriction>
    </simpleType>
    <simpleType name="qualifiedAttributeType">
      <restriction base="xs:string">
        <enumeration value="Ad1"/>
        <enumeration value="Ad2"/>
        <enumeration value="Ad3"/>
      </restriction>
    </simpleType>
  </schema>

```

Listato 14 - federationRegistry.xsd



## 4 TRACCIATURE

### 4.1. TRACCIATURE IDENTITY PROVIDER

Ai fini della tracciatura l'*Identity Provider* dovrà mantenere un *Registro delle transazioni* contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione la tripla composta dall'identificativo dell'identità digitale (*spidCode*) interessata dalla transazione, dalla **<AuthnRequest>** e della relativa **<Response>**. Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi in formato SAML. A titolo esemplificativo e non esaustivo le informazioni presenti in un record del registro potrebbero essere le seguenti:

- **SpidCode;**
- **<AuthnRequest>;**
- **<Response>;**
- **AuthnReq\_ID;**
- **AuthnReq\_IssueInstant;**
- **AuthnReq\_Issuer;**
- **Resp\_ID;**
- **Resp\_IssueInstant;**
- **Resp\_Issuer;**
- **Assertion\_ID;**
- **Assertion\_subject;**
- **Assertion\_subject\_NameQualifier;**

### 4.2. TRACCIATURE SERVICE PROVIDER

Il comma 2 dell'articolo 13 del DPCM obbliga i fornitori di servizi (*service provider*) alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi. A tal fine un *service provider* dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione la coppia dalla **<AuthnRequest>** e della relativa **<Response>**. Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi in formato SAML. A titolo esemplificativo e non esaustivo le informazioni presenti in un record del registro potrebbero essere le seguenti:

- **<AuthnRequest>;**



- < Response>;
- AuthnReq\_ID;
- AuthnReq\_IssueInstant;
- Resp\_ID;
- Resp\_IssueInstant;
- Resp\_Issuer;
- Assertion\_ID;
- Assertion\_subject;
- Assertion\_subject\_NameQualifier;

#### 4.3. MANTENIMENTO TRACCIATURE

Le tracciate devono essere mantenute nel rispetto del codice della privacy sotto la responsabilità titolare del trattamento dell'Identity Provider. e l'accesso ai dati di tracciatura deve essere riservato a personale incaricato.

Al fine di garantire la confidenzialità potrebbero essere adottati meccanismi di cifratura dei dati o impiegati sistemi di basi di dati (DBMS) che realizzano la persistenza cifrata delle informazioni.

Per il mantenimento devono essere messi in atto meccanismi che garantiscono l'integrità e il non ripudio.



## 5 RIFERIMENTI

OASIS	OASIS	<a href="https://www.oasis-open.org/">https://www.oasis-open.org/</a>
SAML	SAML Specifications	<a href="http://saml.xml.org/saml-specifications">http://saml.xml.org/saml-specifications</a>
SAML-Core	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0	<a href="http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf</a>
SAML-Bin	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0	<a href="http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf</a>
SAMLAUTHContext	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	<a href="http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf</a>
SAML-Metadata	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0	<a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a>
SAML-TechOv	SAML Technical Overview	<a href="http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf">http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf</a>
XMLSig	W3C XML Signature WG	<a href="http://www.w3.org/Signature/">http://www.w3.org/Signature/</a>







# MINISTERO DELL'INTERNO

DECRETO 23 dicembre 2015

Modalita' tecniche di emissione della Carta d'identita' elettronica.  
(15A09809)

(GU n.302 del 30-12-2015)

IL MINISTRO DELL'INTERNO  
di concerto con

IL MINISTRO DELL'ECONOMIA E DELLE FINANZE, IL MINISTRO PER LA  
SEMPLIFICAZIONE E LA PUBBLICA AMMINISTRAZIONE

Visto l'art. 3 del regio decreto 18 giugno 1931, n. 773, Testo unico delle leggi di pubblica sicurezza, di seguito TULPS, ed il relativo regolamento di esecuzione del 6 maggio 1940, n. 635;

Vista la legge 13 luglio 1966, n. 559 e in particolare l'art.2, comma 8;

Visto il decreto-legge 31 gennaio 2005, n. 7, convertito con modificazioni in legge 31 marzo 2005, n. 43;

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante "Codice dell'amministrazione digitale";

Visto il decreto del Presidente del Consiglio dei ministri 22 ottobre 1999, n. 437;

Visto il decreto del Ministro dell'interno 23 aprile 2002, istitutivo del Centro nazionale per i servizi demografici presso il Dipartimento per gli Affari interni e territoriali - Direzione centrale per i servizi demografici;

Visto il decreto del Presidente del Consiglio dei ministri 10 novembre 2014, n. 194, recante "modalita' di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente";

Visto l'art. 10, comma 3, del decreto-legge 19 giugno 2015, n. 78, recante "Disposizioni urgenti in materia di enti territoriali" convertito, con modificazioni, dalla legge del 6 agosto 2015, n.125 che prevede che l'emissione della carta d'identita' elettronica e' riservata al Ministero dell'interno che vi provvede nel rispetto delle norme di sicurezza in materia di carte valori, di documenti di sicurezza della Repubblica e degli standard internazionali di sicurezza;

Visto il medesimo art. 10, comma 3, del citato d.l. n. 78 del 2015, che stabilisce che con decreto del Ministro dell'interno, di concerto con il Ministro per la semplificazione e la pubblica amministrazione e il Ministro dell'economia e delle finanze, sentita l'Agenzia per l'Italia digitale, il Garante per la protezione dei dati personali e la Conferenza Stato-citta' autonomie locali, siano definite le caratteristiche tecniche, le modalita' di produzione, di emissione, di rilascio della carta d'identita' elettronica, nonche' di tenuta del relativo archivio informatizzato;

Vista la direttiva 98/34/CE del Parlamento europeo e del Consiglio,

del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata dalla legge 21 giugno 1986, n. 317, modificata dal decreto legislativo 23 novembre 2000, n. 427;

Vista la legge 1° aprile 1999, n. 91, recante "Disposizioni in materia di prelievi e di trapianti di organi e di tessuti";

Visto il decreto del Ministro della sanità dell'8 aprile 2000, recante "Disposizioni in materia di prelievi e di trapianti di organi e di tessuti, attuativo delle prescrizioni relative alla dichiarazione di volontà dei cittadini sulla donazione di organi a scopo di trapianto", come modificato dal decreto del Ministro della salute dell'11 marzo 2008;

Visto il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante "Codice per la protezione dei dati personali";

Visto il decreto del Ministero dell'economia e delle finanze 4 agosto 2003 e successive modificazioni, recante "Nuove istruzioni per la disciplina dei servizi di vigilanza e controllo sulla produzione delle carte valori, degli stampati a rigoroso rendiconto, degli stampati comuni e delle pubblicazioni ufficiali";

Visto il decreto del Ministero dell'economia e delle finanze 23 dicembre 2013 recante "individuazione delle carte valori ai sensi dell'art. 2, comma 10-bis, lettere a) e b) della legge 13 luglio 1966, n. 559 e successive modificazioni e integrazioni";

Sentita l'Agenzia per l'Italia digitale che si è espressa con determinazione n. 169/2015 del 14 dicembre 2015;

Sentito il Garante per la protezione dei dati personali che si è espresso con parere n. 656, in data 17 dicembre 2015;

Sentita la Conferenza Stato-città e autonomie locali in data 17 dicembre 2015;

Decreta:

Art. 1

#### Definizioni

1. Ai sensi del presente decreto si intende per:

a) "ANPR": l'Anagrafe Nazionale della Popolazione Residente, di cui all'articolo 62 del CAD;

b) "Autenticazione in rete": l'identificazione informatica tramite la CIE, ai sensi dell'articolo 64 del CAD, finalizzata all'accesso ai servizi erogati in rete dalle pubbliche amministrazioni;

c) "CA Autenticazione": la struttura di Certification Authority del CNSD che emette i certificati di autenticazione in rete, componente della piattaforma e dell'infrastruttura per l'emissione della CIE;

d) "CAD": il Codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modifiche;

e) "Cartellino elettronico": la trasposizione in formato digitale del cartellino cartaceo di cui all'articolo 290 del regio decreto 6 maggio 1940, n. 635;

f) "Centro Nazionale Trapianti": il Centro nazionale per i trapianti istituito dall'articolo 8 della legge 1 aprile 1999, n. 91, e successive modificazioni;

g) "Certificato di Autenticazione": il certificato digitale rilasciato dalla "CA Autenticazione" necessario per l'autenticazione in rete;

h) "CIE": il documento d'identità personale rilasciato dal Ministero dell'interno denominato "Carta d'Identità Elettronica";

i) "CNSD": il Centro Nazionale dei Servizi Demografici, costituito con il decreto ministeriale 23 aprile 2002, presso il Ministero dell'interno - Dipartimento affari interni e territoriali;

j) "CP-CIE": il centro di produzione della CIE, componente della

piattaforma e dell'infrastruttura per l'emissione della CIE;

k) "Dati di identificazione": i dati memorizzati sul microprocessore ai fini della verifica dell'identita';

l) "Elementi biometrici primari": l'immagine del volto del titolare della CIE, secondo quanto indicato nell'allegato B;

m) "Elementi biometrici secondari": l'immagine delle impronte digitali del titolare della CIE ai sensi dell'art.3 del regio decreto 18 giugno 1931, n.773, secondo quanto indicato nell'allegato B;

n) "PKI-CIE": l'insieme delle infrastrutture a chiave pubblica (Public Key Infrastructure - PKI), delle infrastrutture di comunicazione e pubblicazione dei certificati, costituite da sistemi, entita' e procedure operative preposte a garantire la certificazione dei dati di identificazione contenuti nel microprocessore, la protezione dei dati stessi e la sicurezza del circuito di emissione e controllo della CIE, componente della piattaforma e dell'infrastruttura per l'emissione della CIE;

o) "IPZS": l'Istituto Poligrafico e Zecca dello Stato S.p.A.;

p) "PIN": il codice segreto personale necessario alla fruizione dei servizi che richiedono l'autenticazione in rete;

q) "CIEonline": l'infrastruttura informatica e di rete che rende disponibili i servizi di supporto al processo di emissione e gestione della CIE, componente della piattaforma e dell'infrastruttura per l'emissione della CIE;

r) "Portale": il sito web della CIE, componente della piattaforma e dell'infrastruttura per l'emissione della CIE;

s) "Postazione": l'apparato hardware e software dedicato all'acquisizione dei dati previsti;

t) "PUK": la chiave personale non modificabile di sblocco necessaria alla riabilitazione del PIN a seguito di relativo blocco;

u) "RIPA": la Rete Internazionale delle Pubbliche Amministrazioni;

v) "Sistema Informativo dei Trapianti" o "SIT", il sistema istituito nell'ambito del Sistema Informativo Sanitario Nazionale in base all'articolo 7 della legge 1° aprile 1999, n. 91, che consente la raccolta, in un'unica banca dati, delle manifestazioni di volonta' in tema di donazione degli organi e tessuti espresse dai cittadini;

w) "SPC": il Sistema Pubblico di Connettivita' di cui al CAD;

x) "SSCE": il sistema di servizi del CNSD per il circuito di emissione della CIE, componente della piattaforma e dell'infrastruttura per l'emissione della CIE.

## Art. 2

### Oggetto

1. Il presente decreto definisce le procedure di emissione della CIE determinando le caratteristiche tecniche della piattaforma e dell'architettura logica dell'infrastruttura, disciplinando, altresì, le modalita' tecniche di produzione, distribuzione, gestione e supporto all'utilizzo della CIE.

## Art. 3

### Caratteristiche della CIE

1. La CIE ha le caratteristiche grafiche previste dal modello di cui all'allegato A. Tale modello e' aggiornato con decreto direttoriale del Ministero dell'interno, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali, e pubblicato sul proprio sito istituzionale.

2. Il supporto fisico della CIE e' realizzato con le tecniche tipiche della produzione di carte valori, integrato con un microprocessore per la memorizzazione delle informazioni necessarie

per la verifica dell'identita' del titolare, inclusi gli elementi biometrici primari e secondari, nonche' per l'autenticazione in rete, secondo le caratteristiche tecniche di cui all'allegato B che sono aggiornate con decreto direttoriale del Ministero dell'interno, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali, e pubblicato sul proprio sito istituzionale.

3. Gli elementi biometrici primari e secondari memorizzati nel microprocessore sono utilizzati esclusivamente per verificare l'autenticita' della CIE e l'identita' del titolare attraverso elementi comparativi direttamente disponibili ed escludendo confronti in modalita' "uno a molti" a fini di identificazione.

#### Art. 4

##### Presentazione della richiesta della CIE

La richiesta di rilascio della CIE e' presentata dal cittadino (o dai genitori o tutori in caso di minore) presso l'ufficio anagrafico del Comune di residenza o di dimora, ai sensi dell'articolo 3 del regio decreto 18 giugno 1931, n. 773, o presso il Consolato se cittadino italiano residente all'estero ed iscritto in ANPR

1. residente all'estero, in caso di:

- a) primo rilascio;
- b) smarrimento o furto della CIE o della carta d'identita' in corso di validita', previa presentazione della relativa denuncia;
- c) deterioramento della CIE o della carta d'identita' in corso di validita', previa verifica del relativo stato da parte dell'Ufficiale di anagrafe;
- d) scadenza della carta d'identita'.

2. Il cittadino (o i genitori o i tutori in caso di minori) puo' prenotare la richiesta di rilascio della CIE collegandosi al CIEOnline secondo le modalita' indicate sul Portale.

3. Il Comune o il Consolato, verificata l'identita' del richiedente, accerta l'assenza di eventuali motivi ostativi al rilascio della CIE per il tramite del SSCE, secondo quanto indicato nell'allegato B.

#### Art. 5

##### Acquisizione dei dati del richiedente la CIE

1. Per il rilascio della CIE, il Comune o il Consolato effettua l'acquisizione delle seguenti informazioni del richiedente:

- a) elementi biometrici primari;
- b) elementi biometrici secondari;
- c) firma autografa nei casi previsti;
- d) dato relativo all'autorizzazione o meno all'espatrio;
- e) dato facoltativo relativo alla volonta' di donazione o diniego di organi e/o di tessuti;
- f) eventuali indirizzi di recapito della CIE o di contatto del richiedente per ricevere comunicazioni inerenti allo stato di avanzamento della pratica di rilascio della CIE.

2. Al termine dell'operazione di acquisizione dei dati di cui al comma 1, il Comune o il Consolato rilascia al richiedente la ricevuta della richiesta della CIE, comprensiva del numero della pratica e della prima parte dei codici PIN/PUK associati alla CIE.

#### Art. 6

##### Consegna della CIE

1. La consegna della CIE e della seconda parte dei codici PIN/PUK associati ad essa avviene, entro sei giorni lavorativi, presso l'indirizzo indicato all'atto dell'acquisizione dei dati del richiedente. Per i cittadini italiani residenti all'estero ed iscritti in ANPR la consegna della CIE avverrà secondo le modalità stabilite dall'art. 17 del presente decreto.

#### Art. 7

#### Interdizione dell'operatività della CIE

1. In caso di furto o smarrimento, il cittadino effettua il blocco della propria CIE per inibirne l'utilizzo ai fini dell'accesso ai servizi in rete, contattando il servizio di help desk della CIE e sporge regolare denuncia presso le Forze di Polizia.

#### Art. 8

#### Cartellino elettronico

1. Il cartellino elettronico, conservato da SSCE, contiene le informazioni anagrafiche, la fotografia, la scansione della firma autografa, il numero di protocollo della pratica, le informazioni relative al processo di rilascio e il numero univoco nazionale della CIE.

2. Le Questure accedono alle informazioni contenute nel cartellino elettronico esclusivamente tramite il CNSD.

#### Art. 9

#### Soggetti coinvolti

1. Le funzioni per lo svolgimento delle attività di produzione, distribuzione, gestione e supporto all'utilizzo della CIE vengono svolte dal Ministero dell'interno, dal Ministero dell'economia e delle finanze, dai Comuni, dai Consolati e da IPZS.

2. È istituita, presso il Ministero dell'interno, Dipartimento per gli Affari interni e territoriali - Direzione centrale per i servizi demografici, la Commissione interministeriale permanente della CIE, preposta agli indirizzi strategici e al monitoraggio delle varie fasi del progetto.

#### Art. 10

#### Funzioni del Ministero dell'interno

1. Il Ministero dell'interno, Dipartimento per gli Affari interni e territoriali - Direzione centrale per i servizi demografici, assicura il supporto necessario ai Comuni, ai Consolati e alle Questure per il corretto espletamento delle attività connesse all'attuazione del presente decreto mettendo a disposizione, avendone la responsabilità, l'infrastruttura informatica ubicata nel CNSD che comprende:

- a) il circuito di emissione (SSCE) della CIE;
- b) il sistema finalizzato a garantire l'integrità e la sicurezza delle comunicazioni telematiche tra il CNSD ("sistema di sicurezza del CNSD") ed i vari enti coinvolti nel processo di emissione della CIE secondo quanto indicato nell'allegato B, paragrafo 6, in sostituzione del sistema infrastrutturale previsto dal DM 2 agosto del 2005;
- c) la Certification Authority (CA Autenticazione e PKI-CIE);

- d) il servizio di convalida dei dati anagrafici al CIEonline tramite il collegamento con l'ANPR;
- e) il numero univoco nazionale di inizializzazione della CIE al CP-CIE;
- f) il servizio di validazione dei certificati di autenticazione ai sistemi che erogano servizi on line accessibili tramite la CIE;
- g) il CIEonline;
- h) il Portale;
- i) la banca dati della CIE.

#### Art. 11

#### Funzioni dei Comuni e dei Consolati

1. I Comuni e i Consolati identificano il soggetto richiedente la CIE e, nel rispetto delle regole tecniche e di sicurezza indicate nell'allegato B, ne acquisiscono i dati di cui all'articolo 5, attraverso le apposite postazioni collegate con il CIEonline di cui all'art.12, comma 4, e richiedono la produzione della CIE al Ministero dell'interno, tramite il CNSD.

2. Per lo svolgimento delle attività di competenza nell'ambito del processo di emissione della CIE, eventuali dotazioni hardware aggiuntive devono essere conformi alle caratteristiche tecniche definite dalla Commissione di cui all'art.13.

#### Art. 12

#### Funzioni di IPZS

1. IPZS mette a disposizione del CNSD la piattaforma e l'infrastruttura, di cui all'articolo 2, descritta nell'allegato B, assicurandone la realizzazione, la manutenzione e la conduzione operativa.

2. Per lo svolgimento delle attività connesse all'attuazione del presente decreto, IPZS fornisce al CNSD ed al personale comunale addetto, adeguata documentazione, formazione del relativo personale e supporto tecnico.

3. IPZS fornisce al CNSD gli strumenti necessari per quanto previsto all'articolo 10.

4. IPZS mette a disposizione dei Comuni, dei Consolati e delle Questure un servizio di help desk per fornire il supporto tecnico necessario al corretto espletamento delle attività connesse al rilascio ed al controllo del ciclo di vita della CIE.

5. IPZS mette a disposizione dei cittadini un servizio di help desk telefonico attraverso il quale attivare la procedura di interdizione in caso di smarrimento o furto della CIE secondo quanto indicato nell'allegato B.

6. Per lo svolgimento delle attività di competenza nell'ambito del processo di emissione della CIE, IPZS fornisce ai Comuni le dotazioni hardware e software delle postazioni, conformi alle caratteristiche tecniche definite dalla Commissione di cui all'art.13, nonché i relativi aggiornamenti e i servizi di installazione, di manutenzione e di supporto tecnico e informativo.

7. Il numero di postazioni e la relativa ubicazione sono definite dal Ministero dell'interno.

8. IPZS provvede alla produzione e alla spedizione della CIE secondo quanto previsto dall'articolo 6 e in conformità a quanto stabilito nel decreto del Ministro dell'economia e delle finanze del 4 agosto 2003.

#### Art. 13

## Commissione interministeriale permanente della CIE

1. La Commissione di cui all'articolo 9, comma 2:

a) supporta il Ministero dell'interno nella definizione del piano di graduale avvio del rilascio della CIE presso Comuni e Consolati;

b) verifica lo stato di avanzamento del progetto nei diversi ambiti e aspetti;

c) definisce le modalita' di adozione degli standard tecnologici, delle linee guida e delle specifiche tecniche e delle eventuali funzionalita' aggiuntive, sentito il Garante per la protezione dei dati personali, per i soli aspetti concernenti il trattamento dei dati personali;

d) definisce, sentito il Garante per la protezione dei dati personali, per i soli aspetti concernenti la sicurezza dei dati e del sistema e il trattamento dei dati personali, le caratteristiche tecniche delle dotazioni hardware e software delle postazioni dei Comuni e dei Consolati;

e) garantisce, sentito il Garante per la protezione dei dati personali, per i soli aspetti concernenti la sicurezza dei dati e del sistema e il trattamento dei dati personali, l'aggiornamento e l'allineamento del sistema in relazione all'evoluzione tecnologica, alle direttive europee e alle possibili interazioni con altri sistemi di identificazione elettronica ed altre iniziative governative strategiche di interesse nazionale ed internazionale.

2. La Commissione e' costituita dal Presidente, designato dal Ministero dell'interno, e dai seguenti componenti:

a) un rappresentante del Ministero dell'interno e un supplente;

b) un rappresentante del Ministero dell'economia e delle finanze e un supplente;

c) un rappresentante del Ministero degli esteri e un supplente;

d) un rappresentante designato dal Ministro per la semplificazione e la pubblica amministrazione e un supplente;

e) un rappresentante designato dall'Agenzia per l'Italia digitale e un supplente;

f) un rappresentante designato dall'IPZS e un supplente;

g) un rappresentante designato dall'Associazione Nazionale dei Comuni Italiani (ANCI) e un supplente.

3. Il Presidente e i componenti della Commissione rimangono in carica per un triennio e svolgono il mandato a titolo gratuito. L'incarico e' rinnovabile.

4. Alle sedute della Commissione possono essere invitati a partecipare esperti anche di altre Amministrazioni, Enti e Organismi per gli aspetti tecnologici connessi al progetto.

5. Fino alla costituzione della Commissione di cui al presente articolo i compiti di cui al comma 1 sono svolti dal Gruppo tecnico di lavoro istituito dal Direttore centrale per i servizi demografici del Dipartimento Affari interni e territoriali del Ministero dell'interno.

## Art. 14

### Piano di graduale rilascio della CIE

1. I Comuni che, alla data di entrata in vigore del presente decreto, emettono la carta d'identita' elettronica ai sensi dell'articolo 7-vicies ter del decreto-legge 31 gennaio 2005, n. 7, convertito, con modificazioni, dalla legge 31 marzo 2005, n. 43, avviano il processo di rilascio della CIE secondo le regole tecniche e di sicurezza previste dal presente decreto, nei tempi e nelle modalita' stabilite dalla Commissione di cui all'articolo 13.

2. Nei restanti Comuni e nei Consolati, il rilascio della CIE e' avviato secondo il piano definito dal Ministero dell'interno sentita la Commissione di cui all'articolo 13.



## Art. 15

### Trattamento dei dati personali

1. Ai fini della produzione, del rilascio e della gestione della CIE, il trattamento dei dati personali e' effettuato nel rispetto delle disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196 e successive modifiche.

1. Il Ministero dell'interno - Dipartimento Affari interni e territoriali, il Ministero dell'economia e delle finanze, i Comuni e il Ministero degli affari esteri sono titolari del trattamento di dati personali di propria competenza.

3. Il Ministero dell'interno, le Amministrazioni e gli Enti coinvolti nel processo di emissione non procedono in alcun caso al tracciamento e/o alla registrazione centralizzata di dati relativi all'utilizzo della CIE per l'accesso ai servizi erogati da altri soggetti.

## Art. 16

### Donazione di organi e tessuti

1. Il cittadino maggiorenne, in sede di richiesta al Comune di rilascio della CIE, ha facolta' di indicare il proprio consenso, ovvero diniego, alla donazione di organi e tessuti in caso di morte.

2. L'indicazione di cui al comma 1 e' trasmessa dal comune al Sistema Informativo Trapianti con le modalita' indicate nell'allegato B.

3. Nel caso in cui il cittadino intenda modificare la propria volonta' precedentemente registrata nel SIT, si deve recare presso la propria ASL di appartenenza oppure le aziende ospedaliere o gli ambulatori dei medici di medicina generale o i Centri Regionali per i Trapianti (CRT), o - limitatamente al momento di rinnovo della CIE - anche presso il Comune.

## Art. 17

### Emissione della CIE da parte dei Consolati

1. I Consolati sono autorizzati all'emissione della CIE per i cittadini italiani residenti all'estero che ne fanno richiesta presso gli Uffici consolari stessi.

2. Il Ministro dell'interno e il Ministro degli affari esteri definiscono congiuntamente le modalita' organizzative e tecniche di dettaglio per l'emissione della CIE da parte degli Uffici consolari.

## Art. 18

### Abrogazioni e norme transitorie

1. Il presente decreto sostituisce integralmente il decreto ministeriale 8 novembre 2007.

2. Le carte d'identita' in formato cartaceo ed elettronico rilasciate fino all'emissione della CIE di cui al presente decreto mantengono la propria validita' fino alla scadenza.

## Art. 19

### Clausola di invarianza finanziaria

Le attività del presente decreto saranno realizzate con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il presente decreto, che sarà trasmesso ai competenti organi di controllo, entra in vigore il giorno della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 23 dicembre 2015

Il Ministro dell'interno  
Alfano

Il Ministro dell'economia e delle finanze  
Padoan

Il Ministro per la semplificazione e la pubblica amministrazione  
Madia

Registrato alla Corte dei conti il 30 dicembre 2015  
Interno, registro n. 1, foglio n. 2392

Allegato

Allegato A  
Carta di Identità Elettronica

Allegato B  
Caratteristiche Tecniche della CIE,  
Processo di emissione, Infrastruttura tecnologica e organizzativa

Parte di provvedimento in formato grafico