

LINEE GUIDA OPERATIVE PER LA FRUIZIONE DEI SERVIZI SPID DA PARTE DEI MINORI

Versione 2 in data 11 maggio 2022

Versione	Data	Determinazione	Tipologia modifica
1	2 marzo 2022	Determinazione AgID n. 51 del 2 marzo 2022	Prima emissione
2	11 maggio 2022	Determinazione AgID n. 133 dell'11 maggio 2022	Seconda emissione

Sommario

Capitolo 1	Prefazione.....	4
Capitolo 2	Introduzione.....	5
Capitolo 3	Riferimenti e sigle	8
3.1	Riferimenti normativi.....	8
3.2	Standard di riferimento	9
3.3	Linee guida e Regolamenti di primario riferimento	10
3.4	Termini e definizioni	10
Capitolo 4	Rilascio di SPID ai minori	11
Capitolo 5	Fruibilità dei servizi dedicati ai minori.....	14
5.1	Procedure di fruizione dei servizi dedicati ai minori	14
5.2	Gestione delle sessioni di autenticazione	15
Capitolo 6	Gestione identità del minore e autorizzazioni.....	16
6.1	Autorizzazioni all'accesso	16
6.2	Gestione dell'identità digitale del minore e delle correlate autorizzazioni	16
6.3	Gestione dei <i>log</i> delle autorizzazioni	17
Capitolo 7	Limitazione dell'accesso ai servizi in rete	18
7.1	Metadata SAML IdP.....	18
7.2	Metadata SAML SP	19
7.3	Verifiche effettuate da IdP	22
7.4	Messaggi all'utente	22
Capitolo 8	L'identità al sopraggiungere della maggiore età	23
Capitolo 9	Protezione dei dati personali del minore	24

Capitolo 1

Prefazione

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici la presente linea guida utilizzerà le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «È RICHiesto», «DOVREBBE», «NON DOVREBBE», «RACCOMANDATO», «NON RACCOMANDATO» «PUÒ» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare la linea guida;
- **NON DEVE** o **NON DEVONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **RACCOMANDATO** o **NON DOVREBBE** o **NON RACCOMANDATO**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÒ** o **POSSONO** o l'aggettivo **OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione la specifica.

Capitolo 2

Introduzione

Le presenti Linee guida hanno ad oggetto il rilascio dell'identità digitale in favore dei minori d'età e, pertanto, definiscono:

- le modalità di rilascio dell'identità digitale al minore;
- le modalità di fruizione dei servizi online mediante tale identità.

Nel rispetto della normativa in materia di identità digitale e di protezione dei dati personali nonché delle vigenti Linee guida di primario riferimento in ambito SPID, le presenti Linee guida individuano le modalità operative che i gestori dell'identità digitale e i fornitori di servizi SPID dovranno porre in essere al fine di consentire ai minori la fruizione dei servizi in rete in piena sicurezza.

Con l'identità digitale dei minori si mira a garantire il raggiungimento dei seguenti obiettivi:

1. consentire ai minori di acquisire la propria identità digitale, previa richiesta da parte di chi esercita la responsabilità genitoriale;
2. consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando - salvo casi specifici - la possibilità di autorizzazione e verifica da parte dell'esercente la responsabilità genitoriale;
3. consentire ai fornitori di servizi in rete la selezione dei propri utenti in base all'età.

Più nello specifico, al fine di comprendere la cornice all'interno della quale le presenti Linee guida intendono disciplinare il rilascio e la fruizione dell'identità digitale del minore, risulta fondamentale chiarire alcuni aspetti di primaria rilevanza.

In primo luogo, è necessario evidenziare che l'esercente la responsabilità genitoriale PUÒ chiedere il rilascio dell'identità digitale a favore del minore unicamente al gestore dell'identità digitale presso il quale il medesimo già detiene la propria identità digitale.

In secondo luogo, è essenziale chiarire che, prima di erogare un servizio ai minori mediante SPID, i fornitori di servizi DEVONO effettuare un'autonoma, motivata e dimostrabile valutazione in merito alla necessità di:

- a) conoscere la minore età dell'utente;
- b) ottenere la certezza della sua identità per le finalità del servizio.

In terzo luogo, è opportuno ricordare che l'informativa sul trattamento dei dati personali resa al minore sia da parte del gestore dell'identità digitale sia da parte del fornitore di servizi DEVE essere formulata con un linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile.

È utile precisare sin da subito, inoltre, che, nell'utilizzo dell'identità digitale da parte del minore, occorre distinguere fra:

- l'autorizzazione, espressa dal titolare della responsabilità genitoriale, alla fruizione del servizio da parte del minore;
- il consenso al trattamento dei dati personali, ove richiesto in base all'art. 6, par. 1, lett. a) del RGPD, reso:
 - dal titolare della responsabilità genitoriale, in caso di minore infraquattordicenne;
 - dal minore stesso, al compimento dei quattordici anni.

Su tale base, tuttavia, si innesta il Considerando 86 del RGPD, che richiede una particolare attenzione alla tutela della riservatezza del minore laddove chiarifica che “Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore”.

È alla luce di tali considerazioni che il fornitore di servizi DEVE individuare, sulla base della normativa vigente nonché della tipologia e della finalità del servizio erogato in rete, i casi in cui, avendo ritenuto necessaria l'identificazione del minore per l'accesso al servizio, NON DEVE chiedere all'esercente la responsabilità genitoriale l'autorizzazione all'accesso del minore al servizio, al fine di garantire e tutelare la riservatezza del minore con particolare riferimento ai servizi di prevenzione o consulenza diretta.

A valle di tale valutazione, lasciata inevitabilmente alla responsabilità del fornitore di servizi che eroga lo specifico servizio, questi DEVE utilizzare la procedura corretta fra quelle indicate al successivo Capitolo 5.

Alla luce del parere del Garante per la protezione dei dati personali, emesso ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell'amministrazione digitale, le presenti Linee guida consentono l'utilizzo di SPID, con riferimento ai minori infraquattordicenni, unicamente a partire dai cinque anni e per la fruizione dei soli servizi online erogati dagli istituti scolastici di ogni ordine e grado.

Prima dell'avvio dei trattamenti di dati personali in applicazione delle Linee guida in esame, con appositi e successivi provvedimenti dell'Agenzia, anche con il coinvolgimento del Ministero dell'Istruzione sugli argomenti di comune competenza, saranno individuate adeguate garanzie concernenti i presupposti e le modalità di rilascio di SPID ai minori fra i cinque e i quattordici anni, i trattamenti effettuabili da parte dei gestori dell'identità digitale - limitati a quanto strettamente necessario alla gestione dell'identità - e l'individuazione dei servizi che gli istituti scolastici potranno offrire ai minori infraquattordicenni.

Si specifica infine che, con atto successivo, l'Agenzia disciplinerà altresì l'istituto dell'emancipazione del minore, che attualmente è considerato - ai fini delle presenti Linee guida - quale minore ultraquattordicenne.

Capitolo 3

Riferimenti e sigle

3.1 Riferimenti normativi

La normativa vigente consente la creazione dell'identità digitale in favore di tutti i cittadini.

Risulta evidente, tuttavia, la necessità di una tutela specifica per un soggetto fragile come il minore. Per tale ragione si è proceduto ad analizzare le principali disposizioni normative unionali e nazionali con riferimento alla sfera giuridica e alla riservatezza del minore.

Con riferimento alla normativa vigente in tema di protezione dei dati personali, è essenziale rapportare le presenti Linee guida operative *in primis* al Regolamento (UE) 2016/679 recante il Regolamento Generale sulla Protezione dei Dati (di seguito RGPD).

Il Considerando 38 del RGPD stabilisce quanto segue: *“I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore”*.

L'articolo 8 del RGPD, con riferimento al trattamento dei dati personali del minore in relazione ai servizi della società dell'informazione, chiarisce che il trattamento effettuato sulla base del consenso del minore è lecito *“[...] ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. *Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. [...]*”.

Il legislatore italiano, mediante il decreto legislativo 10 agosto 2018, n. 101, ha introdotto nel decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati

personali l'articolo 2-quinquies rubricato “*Consenso del minore in relazione ai servizi della società dell'informazione*”. In virtù di tale disposizione “[...] il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguarda.”

Per quanto concerne la sfera giuridica del minore nell'ordinamento italiano, il codice civile è certamente il riferimento primario. Il primo comma dell'articolo 320 del codice civile dispone che “I genitori congiuntamente, o quello che esercita in via esclusiva la responsabilità genitoriale, rappresentano i figli nati e nascituri, fino alla maggiore età o all'emancipazione, in tutti gli atti civili e ne amministrano i beni. Gli atti di ordinaria amministrazione, esclusi i contratti con i quali si concedono o si acquistano diritti personali di godimento, possono essere compiuti disgiuntamente da ciascun genitore.

Si applicano, in caso di disaccordo o di esercizio difforme dalle decisioni concordate, le disposizioni dell'articolo 316. [...]”.

In considerazione di quanto sopra e, più in generale, della normativa vigente con riferimento alla sfera giuridica del minore e alla protezione dei suoi dati personali, l'accesso ai servizi in rete da parte di quest'ultimo necessita di valutazioni sulla base dei seguenti criteri:

- l'età del minore;
- la tipologia e la finalità del servizio richiesto.

3.2 Standard di riferimento

- [SAML] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0: <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.

3.3 Linee guida e Regolamenti di primario riferimento

- **[RT_SPID]** *“Regolamento recante le regole tecniche”, adottato con determinazione n. 44 del 28 luglio 2015, ai sensi dell’articolo 4, comma 2, del decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante “Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese”;*
- **[MAR_SPID]** *“Regolamento recante le modalità attuative per la realizzazione dello SPID”, adottato con determinazione n. 44 del 28 luglio 2015, ai sensi dell’articolo 4, comma 2, del decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante “Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese”.*

3.4 Acronimi e definizioni

Di seguito si riportano gli acronimi e le definizioni che verranno utilizzati nelle presenti Linee Guida:

- **[AgID]** Agenzia per l’Italia Digitale
- **[CAD]** D. Lgs. 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell’Amministrazione Digitale
- **[IdP]** Il gestore dell’identità digitale SPID
- **[SP]** Il fornitore di servizi SPID
- **[Genitore]** Il soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio di SPID in favore di quest’ultimo
- **[Genitore non richiedente]** Altro soggetto che esercita la responsabilità genitoriale sul minore
- **[Notifica]** Messaggio che l’IdP invia al Genitore su richiesta del minore.

Capitolo 4

Rilascio di SPID ai minori

Di seguito si illustra la procedura volta al rilascio di SPID in favore del minore:

1. L'IdP offre ai propri utenti un servizio dedicato alla richiesta di rilascio di SPID in favore dei minori e rende apposita informativa sul trattamento dei dati personali del minore per il rilascio e la gestione dell'identità digitale, ai sensi degli artt. 12 e ss. del RGPD.
2. Il Genitore:
 - a. accede, con credenziali di livello 2, al servizio reso disponibile dal proprio IdP;
 - b. inserisce i seguenti dati relativi al minore in favore del quale intende chiedere il rilascio di SPID: nome, cognome, codice fiscale, data nascita;
 - c. dichiara, ai sensi dell'art. 46, comma 1, lett. u) del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i., la propria qualità di esercente la responsabilità genitoriale sul minore;
 - d. accetta la ricezione di notifiche (ordinarie o push) da parte dell'IdP per l'autorizzazione all'utilizzo di SPID da parte del minore.
3. L'IdP:
 - a. genera il *codice del genitore*, composto dal risultato della funzione CRC-32 applicato al codice fiscale del Genitore (ad es.: il codice fiscale RSSMTT64A01G201K produce il CRC 0x4DFCE69E, pertanto il *codice del genitore* sarà 4DFCE69E);
 - b. genera il *codice di verifica* assegnato al minore (univoco nell'ambito di ogni IdP), associando al *codice del genitore* un codice casuale di tre numeri in notazione decimale (seriale minore); ad es.: ipotizzando che il codice casuale sia 737, il *codice di verifica* sarà 4DFCE69E737;
 - c. comunica il *codice di verifica* al Genitore.
4. Il Genitore comunica al minore il *codice di verifica* al di fuori dei canali dell'IdP.
5. Il minore comunica il *codice di verifica* all'IdP scelto dal proprio Genitore, mediante il servizio da questi reso disponibile.
6. L'IdP:

- a. verifica la presenza dell'autorizzazione del Genitore al rilascio di SPID e, in caso positivo:
- b. identifica il minore attraverso le modalità definite all'articolo 7 del D.P.C.M. 24 ottobre 2014 recante *“Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese”* e secondo quanto disposto nel *“Regolamento recante le modalità attuative per la realizzazione dello SPID”*, verificando la corrispondenza della sua identità con i dati precedentemente forniti dal Genitore nonché, quando presente, con il nome di questi sul documento di identità del minore (richiesto durante l'identificazione secondo le modalità prescelta) o mediante le verifiche di cui all'art. 12 del *“Regolamento recante le modalità attuative per la realizzazione dello SPID”*. Fra i documenti verificabili si indicano, a titolo esemplificativo, il certificato di stato di famiglia con rapporti di parentela, il decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l'affidamento del minore. Qualora l'identificazione del minore intervenga *de visu* (in presenza o in modalità informatica), il minore infraquattordicenne DEVE essere affiancato dal Genitore;
- c. rilascia l'identità digitale al minore;
- d. invia una notifica al Genitore, recante l'indicazione del nome del minore per il quale è stato rilasciato lo SPID.

Si chiarisce che, prima del rilascio dell'identità digitale al minore, l'IdP è in ogni caso tenuto ad acquisire dal Genitore e a caricare a sistema:

- dichiarazione, ai sensi dell'art. 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i., di essere autorizzato alla richiesta di SPID da parte dell'eventuale Genitore non richiedente o di essere l'unico esercente la responsabilità genitoriale sul minore;
- copia di documentazione a conferma di quanto dichiarato: documento di identità in corso di validità dell'eventuale Genitore non richiedente o copia di un documento che attesti la dichiarazione di essere l'unico esercente la responsabilità genitoriale (es. stato di morte dell'altro genitore, nomina in qualità di tutore, ecc.).

Con riferimento alla fase di identificazione del minore di cui al precedente punto 6, lett. b), si specifica che gli attributi richiesti al minore sono i seguenti:

- attributi identificativi obbligatori: cognome e nome, sesso, data e luogo di nascita, codice fiscale, estremi di un valido documento di identità, ai sensi dell'art. 1, comma 1, lett. c) del D.P.C.M. 24 ottobre 2014 e all'art. 5, terzo capoverso del “Regolamento recante le modalità attuative per la realizzazione dello SPID”;
- attributi secondari obbligatori: e-mail;
- attributi secondari facoltativi: il domicilio fisico, il domicilio digitale e il numero di telefono mobile (previsto come attributo facoltativo ai fini delle presenti Linee guida, in deroga all'art. 5, quinto capoverso del “Regolamento recante le modalità attuative per la realizzazione dello SPID”).

Nei casi in cui il minore non sia in possesso di un numero di telefonia mobile e/o di un dispositivo mobile, l'eventuale secondo fattore di autenticazione, funzionale alle autenticazioni di livello SPID 2, sarà - a mero titolo esemplificativo - trasmesso su canali alternativi quali l'indirizzo di posta elettronica oppure generato attraverso un apposito dispositivo fisico rilasciato al minore.

Resta ferma, in tali casi, la facoltà dell'IdP di associare all'identità del minore il numero di telefono mobile del Genitore, utilizzabile unicamente per le funzionalità di gestione della sicurezza dell'identità digitale del minore (alert di sicurezza, procedure di recupero delle credenziali, configurazione dell'app di autenticazione, processi di sospensione/revoca, processi di assistenza per ragioni di sicurezza). È sempre escluso l'utilizzo del telefono del Genitore per l'invio del secondo fattore di autenticazione con riferimento all'accesso del minore ai servizi degli SP con livello SPID 2.

Capitolo 5

Fruibilità dei servizi dedicati ai minori

5.1 Procedure di fruizione dei servizi dedicati ai minori

Alla luce di quanto esplicito nell'Introduzione delle presenti Linee guida, di seguito si illustrano le due distinte procedure previste per la fruizione dei servizi in rete da parte dei minori mediante SPID.

5.1.1. Procedura A

La presente procedura si applica nei casi in cui il SP, sulla base della valutazione effettuata con riferimento alla tipologia e alla finalità del servizio erogato, NON DEVE richiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore, in relazione ai servizi erogati dagli istituti scolastici di ogni ordine e grado nonché ai servizi di prevenzione o di consulenza forniti direttamente al minore:

1. il minore chiede l'accesso al servizio del SP;
2. il SP invia all'IdP la richiesta di autenticazione, come da successivo Capitolo 7;
3. l'IdP effettua la procedura di autenticazione del soggetto minore, comprendente anche la *verifica di congruenza* fra l'età richiesta dal SP e l'età effettiva del minore: qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, l'IdP porta a termine il processo di autenticazione del minore presso il SP.

5.1.2. Procedura B

La presente procedura si applica nei casi in cui il SP, sulla base della valutazione effettuata con riferimento alla tipologia e alla finalità del servizio erogato, DEVE richiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore.

Atteso che i minori infraquattordicenni possono accedere unicamente ai servizi online resi disponibili dagli istituti scolastici e che tale accesso è inserito fra quelli di cui alla precedente

Procedura A, la presente Procedura B si applica ai soli minori ultraquattordicenni nell'accesso ai servizi non ricompresi fra quelli di prevenzione o di consulenza forniti direttamente al minore:

1. il minore chiede l'accesso al servizio del SP;
2. il SP invia all'IdP la richiesta di autenticazione, come da successivo Capitolo 7;
3. L'IdP effettua la procedura di autenticazione del soggetto minore, comprendente anche le seguenti operazioni:
 - 3.1. l'IdP esegue la *verifica di congruenza* fra l'età richiesta dal SP e l'età effettiva del minore: qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, l'IdP continua la procedura di autenticazione;
 - 3.2. l'IdP invia al minore la richiesta di conferma della sua volontà di chiedere al Genitore l'autorizzazione all'accesso: qualora il minore non confermi tale volontà, la procedura di autenticazione è interrotta con esito negativo; qualora invece il minore confermi tale volontà, la procedura di autenticazione prosegue con i passaggi successivi;
 - 3.2. l'IdP invia al Genitore una notifica contenente:
 - a. il nome e il cognome del minore;
 - b. la denominazione del SP al cui servizio il minore ha chiesto di accedere;
 - c. la data e l'ora della richiesta di accesso;
 - d. la richiesta di autorizzazione all'accesso del minore;
 - 3.3. qualora il Genitore non autorizzi l'accesso, la procedura di autenticazione è interrotta con esito negativo; qualora invece il Genitore fornisca l'autorizzazione all'accesso, l'IdP porta a termine il processo di autenticazione del minore presso il SP.

5.2 Gestione delle sessioni di autenticazione

In deroga a quanto previsto dall'art. 28 del “*Regolamento recante le modalità attuative per la realizzazione dello SPID*”, al fine di garantire la massima sicurezza e la massima protezione dei dati del minore, è esclusa la possibilità di mantenimento di sessioni condivise di autenticazione per tutti i livelli di SPID. laddove l'accesso al servizio sia permesso anche ai minori.

Capitolo 6

Gestione identità del minore e autorizzazioni

6.1 Autorizzazioni all'accesso

L'IdP DEVE consentire al Genitore di autorizzare l'accesso ai servizi richiesti dal minore entro 24 ore dalla richiesta, mediante il servizio di cui al successivo paragrafo 6.2.

Se, in occasione di un precedente accesso, il Genitore ha già fornito l'autorizzazione, l'IdP autentica nuovamente il minore senza chiedere una nuova autorizzazione.

Il Genitore PUÒ autorizzare l'accesso del minore al servizio indicando all'IdP la durata di tale autorizzazione. Trascorsa tale durata, in presenza di una nuova richiesta di accesso al servizio da parte del minore, l'IdP DEVE chiedere nuovamente l'autorizzazione al genitore.

Ogni autorizzazione decade al momento del decadere dell'identità digitale del Genitore.

Il SP è tenuto a ripetere le procedure di cui al paragrafo 5.1 o al paragrafo 5.2 qualora modifichi le finalità del trattamento dei dati personali e/o le condizioni di erogazione dei servizi.

6.2 Gestione dell'identità digitale del minore e delle correlate autorizzazioni

L'IdP DEVE fornire al Genitore un servizio, accessibile mediante credenziali SPID almeno di livello 2, che consenta:

- la gestione delle identità digitali dei minori associate al Genitore e che preveda almeno la possibilità di sospensione e revoca di tali identità digitali;
- la gestione delle autorizzazioni di accesso ai servizi rilasciate dal Genitore e che preveda almeno la possibilità di sospensione e revoca di tali autorizzazioni.

L'IdP DEVE consentire al Genitore di accedere esclusivamente alle informazioni necessarie all'espletamento di tali attività, garantendo la riservatezza del minore con riferimento a ulteriori informazioni di utilizzo della propria identità digitale.

Nel caso in cui il minore sia ultraquattordicenne, l'IdP DEVE fornire anche a questi un servizio, accessibile mediante credenziali SPID almeno di livello 2, che consenta:

- la gestione, in autonomia, della propria identità digitale e che preveda almeno la possibilità di sospensione di tale identità;
- la consultazione, in autonomia, degli accessi effettuati presso i SP.

6.3 Gestione dei *log* delle autorizzazioni

Ferme restando le disposizioni relative alla gestione dei *log* previste nelle regole tecniche SPID, gli IdP DEVONO conservare i *log* di ogni autorizzazione per un tempo pari a 24 mesi.

I *log* DEVONO contenere unicamente le informazioni di cui alla notifica con la relativa indicazione temporale nonché la risposta del Genitore con la relativa indicazione temporale.

Capitolo 7

Limitazione dell'accesso ai servizi in rete

7.1 Metadata SAML dell'IdP

Il metadata SAML dell'IdP che supporta il servizio di cui alle presenti Linee Guida contiene, all'interno dell'elemento **Extensions**, l'elemento, con *namespace* spid¹:

- **SupportedAgeLimit** - Tag vuoto, *obbligatorio*.

```
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:spid="https://spid.gov.it/saml-extensions"
  [...]>
  <ds:Signature>
    [...]
  </ds:Signature>
  [...]
  <md:Extensions>
    <spid:SupportedAgeLimit />
    [...]
  </md:Extensions>
  <md:IDPSSODescriptor [...]>
    [...]
  </md:IDPSSODescriptor>
  <md:Organization>
    [...]
  </md:Organization>
</md:EntityDescriptor>
```

¹ Il *namespace* spid è definito al valore: <https://spid.gov.it/saml-extensions>.

7.2 Metadata SAML del SP

Il metadata SAML del SP che espone un servizio rivolto ai minori (o anche ai minori) contiene, all'interno dell'elemento **Extensions**, l'elemento con *namespace* spid²:

- **AgeLimit** – (1 occorrenza, *obbligatorio*) contenente i seguenti elementi:
 - **AssertionConsumerServiceIndex** – *obbligatorio*, numero intero corrispondente al valore dell'attributo **index** dell'elemento **AssertionConsumerService**, presente all'interno dello stesso metadata relativo al servizio rivolto ai minori a cui i parametri dell'estensione fanno riferimento.
 - **MinAge** – *obbligatorio*, numero intero indicante l'età minima, espressa in anni, per l'accesso al servizio. Il valore deve essere compreso tra il valore minimo “5” e il valore massimo “17”.
 - **MaxAge** – *obbligatorio*, numero intero indicante l'età massima, espressa in anni, per l'accesso al servizio. Il valore deve essere compreso tra il valore minimo pari al valore indicato in **MinAge** e il valore massimo “999”, ad indicare nessun limite di età.
 - **AgeParentAuth** – *obbligatorio*, numero intero indicante l'età, espressa in anni, al di sotto della quale il SP DEVE chiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore. Il valore deve essere maggiore del valore indicato per **MinAge** e minore di “18”. Se l'autorizzazione del Genitore non è necessaria, l'elemento DEVE essere valorizzato a “0”.

Alcuni esempi:

- a) Per indicare che il servizio, relativo all'AssertionConsumerService identificato da index “1”, è riservato a chi ha 17 anni con richiesta di autorizzazione del Genitore:

² Il *namespace* spid è definito al valore: <https://spid.gov.it/saml-extensions>.

```
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:spid="https://spid.gov.it/saml-extensions" [...]>
  <ds:Signature>
    [...]
  </ds:Signature>
  [...]
  <md:Extensions>
    <spid:AgeLimit>
      <AssertionConsumerServiceIndex>1</AssertionConsumerServiceIndex>
      <MinAge>17</MinAge>
      <MaxAge>17</MaxAge>
      <AgeParentAuth>18</AgeParentAuth>
    </spid:AgeLimit>
    [...]
  </md:Extensions>
  <md:SPSSODescriptor [...]>
    [...]
    <md:AssertionConsumerService [...] index="1" />
    [...]
  </md:SPSSODescriptor>
  [...]
</md:EntityDescriptor>
```

- b) Per indicare che il servizio, relativo all'AssertionConsumerService identificato da index "2", è riservato a chi ha compiuto 13 anni e non ne ha ancora compiuti 16 e che il SP non è tenuto a chiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore che ha compiuto 15 anni:

```
<md:EntityDescriptor [...]>
  [...]
  <md:Extensions>
    <spid:AgeLimit>
      <AssertionConsumerServiceIndex>2</AssertionConsumerServiceIndex>
      <MinAge>13</MinAge>
      <MaxAge>15</MaxAge>
      <AgeParentAuth>15</AgeParentAuth>
    </spid:AgeLimit>
    [...]
  </md:Extensions>
  [...]
</md:EntityDescriptor>
```

- c) Per indicare che il servizio, relativo all'AssertionConsumerService identificato da index "3", è riservato a chi ha compiuto 12 anni e non ha limiti di età e che il SP è sempre tenuto a chiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore:

```
<md:EntityDescriptor [...]>
  [...]
  <md:Extensions>
    <spid:AgeLimit>
      <AssertionConsumerServiceIndex>3</AssertionConsumerServiceIndex>
      <MinAge>12</MinAge>
      <MaxAge>999</MaxAge>
      <AgeParentAuth>18</AgeParentAuth>
    </spid:AgeLimit>
    [...]
  </md:Extensions>
  [...]
</md:EntityDescriptor>
```

Se nel metadata SAML del SP esiste un elemento `AssertionConsumerService` il cui valore dell'attributo `index` non è riportato come valore dell'elemento `AssertionConsumerServiceIndex` in nessuno degli elementi `spid:AgeLimit` eventualmente presenti all'interno dell'elemento `Extensions` del metadata, l'accesso al servizio indirizzato da tale `AssertionConsumerService` è da intendersi consentito soltanto agli utenti maggiorenni.

7.3 Verifiche in capo all'IdP

Per consentire l'accesso a un servizio della società dell'informazione destinato ai minori (o a minori entro un range di età determinato dal SP), l'IdP DEVE:

1. rilevare dal metadata del SP se il servizio a cui è richiesto l'accesso è un servizio destinato ai minori ovvero se esiste un elemento **spid:AgeLimit** il cui valore dell'elemento **AssertionConsumerServiceIndex** corrisponde al valore dell'attributo **index** relativo all'**AssertionConsumerService** cui fa riferimento la richiesta di autenticazione;
2. nel caso in cui si tratti di una richiesta di autenticazione per un servizio destinato ai minori, verificare che l'età dell'utente che sta eseguendo l'autenticazione rientri nell'intervallo identificato dai parametri **MinAge** - **MaxAge**;
3. nel caso in cui l'età dell'utente che sta eseguendo l'autenticazione risulti inferiore all'età indicata nel parametro **AgeParentAuth**, verificare che l'autorizzazione del Genitore sia stata concessa, nel rispetto di quanto previsto nel capitolo 5.

7.4 Messaggi all'utente

Nel caso in cui il minore non sia stato autorizzato all'accesso al servizio richiesto, l'IdP DEVE mostrare il seguente messaggio: *“Spiacente %Nome%, ma non sei autorizzato ad accedere al servizio”*, dove “%Nome%” è il nome proprio del soggetto autenticato.

Nel caso in cui l'età del soggetto non coincida con la richiesta pervenuta dal SP, l'IdP DEVE informare l'utente mediante il seguente messaggio: *“Spiacente %Nome%, ma non hai l'età richiesta da %SP% per accedere al servizio”*, dove “%Nome%” è il nome proprio del soggetto autenticato e “%SP%” è l'indicazione del SP.

Capitolo 8

L'identità al sopraggiungere della maggiore età

Al compimento del diciottesimo anno di età dell'interessato, l'IdP DEVE:

- rimuovere le limitazioni precedentemente imposte dalla minore età;
- eliminare i legami con l'identità digitale del Genitore;
- cancellare tutte le informazioni relative all'utilizzo dell'identità digitale del minore rese disponibili al Genitore, fatta eccezione per i *log*, in ragione del dovuto rispetto della politica di *data retention*;
- inviare un messaggio al neo maggiorenne mettendo a sua disposizione un servizio per dichiarare, previa autenticazione con credenziali SPID di livello 2, di voler mantenere attiva o revocare la propria identità digitale. Sino a che il neo maggiorenne non dichiari esplicitamente, mediante tale servizio, la propria volontà di continuare a usare la propria identità digitale, la fruizione dei servizi mediante SPID è totalmente preclusa. Decorsi due anni dall'ultimo utilizzo dell'identità digitale, questa è automaticamente revocata, in ossequio alla regolamentazione SPID.

Capitolo 9

Protezione dei dati personali del minore

Le presenti Linee guida sono esplicitamente orientate all'applicazione in concreto dei principi fondanti la protezione dei dati personali di cui all'art. 5 del RGPD.

In particolare, le procedure individuate per il rilascio e la gestione dell'identità digitale del minore e per la fruizione dei servizi mediante SPID sono fondate sui principi di liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati rispetto alle finalità individuate; esattezza e aggiornamento dei dati; limitazione della conservazione; integrità e riservatezza, nel rispetto del principio di responsabilizzazione posto in capo all'IdP e al SP, nei contesti di rispettiva competenza e titolarità nel trattamento dei dati personali del minore.

Proprio in tale ottica di primaria attenzione alla protezione dei dati personali del minore, SPID permette ai SP - qualora lo ritengano opportuno in base alle proprie valutazioni, nel rispetto del principio di responsabilizzazione - di ottenere la certezza sull'età del minore anche in assenza di alcun altro dato che possa ulteriormente identificarlo, ad esempio permettendo al SP di richiedere esclusivamente l'attributo che attesta la data di nascita del minore.

SPID, invero, è uno strumento che può essere utilizzato anche per proteggere i minori, in quanto consente l'accesso ai servizi in rete mediante selezione dei relativi fruitori in base all'età o, come sopra indicato, eventualmente anche in modalità anonima.