Presidenza del Consiglio dei Ministri

Dipartimento per la trasformazione digitale

DECRETO

Aggiornamento degli Allegati 1, 3, 4 e 5 al decreto 23 febbraio 2026 recante "Disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe"

IL CAPO DEL DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale e, in particolare, l'articolo 64-ter, che istituisce la Piattaforma di gestione deleghe;

Visto il decreto 23 febbraio 2026, recante "Disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe" e, in particolare, l'articolo 11, comma 3, ai sensi del quale gli aggiornamenti delle specifiche tecniche contenute nell'Allegato 5 sono adottati con decreto del Capo del Dipartimento per la trasformazione digitale, sentito il Garante per la protezione dei dati personali, e con il medesimo decreto sono aggiornati gli Allegati da 1 a 4, ove necessario in conseguenza delle modifiche all'Allegato 5;

Visti, altresì, l'articolo 9, comma 6, del predetto decreto, relativo all'ambito di operatività delle deleghe per i servizi in rete afferenti al Fascicolo sanitario elettronico, all'Ecosistema dati sanitari e alla Piattaforma nazionale di telemedicina;

Visto il decreto del Ministro della salute 7 settembre 2023, recante "Fascicolo sanitario elettronico 2.0";

Visto il decreto del Ministro della salute 31 dicembre 2024, recante "Istituzione dell'Ecosistema dati sanitari";

Visto il decreto del Ministro della salute 19 novembre 2025, recante "Disciplina del trattamento dei dati personali nell'ambito della infrastruttura della Piattaforma nazionale telemedicina";

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

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Visto il Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183, relativo all'istituzione del quadro europeo per l'identità digitale;

Visto il decreto del Segretario generale del 24 luglio 2019, con cui è disciplinata l'organizzazione interna del Dipartimento per la trasformazione digitale, modificato dal decreto del Ministro per l'innovazione tecnologica e la digitalizzazione 3 settembre 2020, registrato dalla Corte dei conti in data 21 settembre 2020 al n. 2159;

Visto il decreto del Presidente della Repubblica del 31 ottobre 2022, con il quale il Sen. Alessio Butti è stato nominato Sottosegretario di Stato alla Presidenza del Consiglio dei ministri;

Visto il decreto del Presidente del Consiglio dei ministri del 25 novembre 2022, concernente la delega di funzioni in materia di innovazione tecnologica e transizione digitale al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, Sen. Alessio Butti;

Visto il decreto del Presidente del Consiglio dei ministri 24 novembre 2022, con il quale al Dott. Angelo Borrelli è stato conferito, ai sensi degli articoli 18 e 28 della legge 23 agosto 1988, n. 400, nonché dell'art. 19 del decreto legislativo 30 marzo 2001, n. 165, l'incarico di Capo Dipartimento per la Trasformazione Digitale;

Considerata la necessità di assicurare l'allineamento costante delle specifiche tecniche di integrazione della Piattaforma alle evoluzioni tecnologiche e alla normativa di settore, rafforzando l'interoperabilità, la sicurezza, la tracciabilità e la protezione dei dati personali nei flussi tra la Piattaforma, i gestori dell'identità digitale e le pubbliche amministrazioni erogatrici dei servizi;

Tenuto conto delle esigenze emerse in relazione all'utilizzo delle deleghe nell'ambito dei servizi del Fascicolo sanitario elettronico, dell'Ecosistema dati sanitari e della Piattaforma nazionale di telemedicina, anche ai fini di una maggiore granularità dei relativi livelli di operatività;

Considerato che l'aggiornamento dell'Allegato 5 rende necessario il conseguente adeguamento degli Allegati 1, 3 e 4, al fine di assicurarne la coerenza con le specifiche tecniche di integrazione aggiornate e con i connessi processi di gestione e utilizzo della delega;

Sentito il Garante per la protezione dei dati personali, che ha reso il parere di competenza con provvedimento del 20 ottobre 2026, acquisito a protocollo DTD-0006907-A-23/10/2026;

DECRETA

Art. 1

(Aggiornamento delle specifiche tecniche e degli allegati)

1. Ai sensi dell'articolo 11, comma 3, del decreto 23 febbraio 2026, sono aggiornate le specifiche tecniche di integrazione contenute nell'Allegato 5 al medesimo decreto. L'Allegato 5 è sostituito dall'Allegato 5 annesso al presente decreto.

2. In conseguenza delle modifiche di cui al comma 1 e al fine di assicurare la coerenza complessiva della disciplina tecnica della Piattaforma, sono altresì aggiornati gli Allegati 1, 3 e 4 al decreto 23 febbraio 2026, che sono sostituiti dai corrispondenti Allegati 1, 3 e 4 annessi al presente decreto.

3. L'Allegato 2 al decreto 23 febbraio 2026 resta invariato.

4. Gli Allegati 1, 3, 4 e 5 annessi al presente decreto ne costituiscono parte integrante e, a decorrere dalla data di efficacia del presente decreto, sostituiscono a ogni effetto i corrispondenti allegati al decreto 23 febbraio 2026.

Art. 2

(Clausola di invarianza)

1. All'attuazione del presente decreto si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

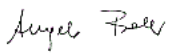
Art. 3

(Entrata in vigore)

1. Il presente decreto entra in vigore il giorno successivo alla sua pubblicazione sul sito internet www.governo.it.
2. Della pubblicazione del presente decreto è dato avviso nella Gazzetta Ufficiale della Repubblica italiana.

IL CAPO DEL DIPARTIMENTO

Angelo Borrelli



27-10-2026 | 15:38:08 CET

CORTE DEI CONTI

UFFICIO DI CONTROLLO SUGLI ATTI DELLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI, DEL MINISTERO DELLA GIUSTIZIA E DEL MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE

Si attesta che il provvedimento numero SN del 27/10/2026, con oggetto PRESIDENZA_Dipartimento per la trasformazione digitale - Aggiornamento degli Allegati 1, 3, 4 e 5 al decreto 23 febbraio 2026 recante “Disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe” pervenuto a questo Ufficio di controllo di legittimità, è stato protocollato in arrivo con prot. n. CORTE DEI CONTI - SCEN_LEA - SCCLA - 0062359 - Ingresso - 03/11/2026 - 07:43 ed è stato ammesso alla registrazione il 16/11/2026 n. 2953

Il Magistrato Istruttore
DONATO CENTRONE
(Firmato digitalmente)

ALLEGATO 1

“Presentazione della delega con l'assistenza remota del Gestore della Piattaforma”

PIATTAFORMA DI GESTIONE DELEGHE

(Art. 4 - Presentazione della delega con l'assistenza remota del Gestore della Piattaforma)

La presentazione della delega di cui all'articolo 64-ter del CAD può essere effettuata mediante il servizio di assistenza remota (web meeting) del Gestore della Piattaforma, dai cittadini iscritti nell'ANPR di età pari o superiore ai 65 (sessantacinque) anni o in possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104.

Il servizio di assistenza remota prevede la presentazione della delega da remoto, tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196. Il Gestore della Piattaforma implementa un sistema che garantisce, preliminarmente all'instaurazione della sessione audio/video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente. Garantisce inoltre l'utilizzo di applicativi orientati all'usabilità e all'accessibilità da parte dell'utente.

La presentazione della delega mediante il servizio di assistenza remota prevede l'identificazione del soggetto delegante e delegato da remoto mediante una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento della delega nel rispetto delle seguenti condizioni:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione degli interlocutori 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 delegante, del delegato e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

Il Gestore della Piattaforma valuta la sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di presentazione della delega nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire le verifiche dell'identità dei soggetti e della volontà di delega.

L'operatore che acquisisce la delega effettua l'identificazione dei soggetti (delegante e delegato) accertandone l'identità tramite la verifica dei rispettivi documenti d'identità in corso di validità, purché muniti di fotografia recente riconoscibile e firma autografa e ne verifica il codice fiscale tramite la tessera sanitaria in corso di validità.

L'operatore può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza dei documenti presentati dai soggetti (delegante e delegato). La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca della delega con modalità crittografiche atte a garantirne l'accesso esclusivamente all'autorità giudiziaria, al gestore della piattaforma e ai soggetti delegante e delegato in caso di disconoscimento della stessa.

Il Gestore della Piattaforma deve richiedere il consenso al trattamento dei dati personali contenuti nelle riprese audio/video.

Il processo di erogazione del servizio è di seguito riportato:

1. Il cittadino delegante (di età pari o superiore ai 65 anni o in possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104) fornisce copia del documento d'identità, del proprio codice fiscale;
2. Il cittadino delegato:
    a. accede al Portale mediante l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo;

    b. carica sul Portale i documenti forniti dal delegante, la copia del documento d'identità, la copia del proprio codice fiscale.
3. La piattaforma (in modo automatico) verifica:
    a. che il delegante ed il delegato siano iscritti in ANPR;
    b. il possesso dei requisiti per l'erogazione del servizio da parte del delegante; per la verifica del possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 il Gestore verifica i relativi servizi INPS mediante PDND.
4. All'esito positivo delle sopracitate verifiche, Il cittadino delegato richiede un appuntamento per l'erogazione del servizio, selezionando una tra le date e orario disponibili;
5. La delega è registrata sul Portale a seguito della conclusione con esito positivo dell'erogazione del servizio e della successiva accettazione da parte del delegato.

L'erogazione del servizio, nella data e orario selezionati, deve essere condotta seguendo una procedura scritta e pubblicata dal Gestore della Piattaforma sul Portale ai Cittadini, che preveda almeno le seguenti attività:

- l'operatore effettua una video chiamata con delegato e delegante
- l'operatore, previa informativa, acquisisce dal delegante e delegato l'assenso alla videoregistrazione e alla sua conservazione. L'operatore informa che la videoregistrazione sarà conservata in modalità protetta fino ad 1 anno dopo la scadenza o revoca della delega, salvo contenziosi;
- l'operatore dichiara i propri dati identificativi;
- l'operatore verifica i documenti caricati;
- i soggetti delegante e delegato confermano le proprie generalità;
- il soggetto delegato dichiara di non possedere le seguenti qualifiche nei confronti del soggetto delegante:
    - esercente la responsabilità genitoriale,
    - tutore, curatore e amministratore di sostegno;
- il soggetto delegato conferma la data e l'ora della registrazione;
- il soggetto delegante esprime in piena consapevolezza la propria volontà di delega;
- l'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere, in generale, al delegato elencando le due opzioni di scelta possibili:
    - Nessun accesso [l'opzione è disponibile nel caso in cui il delegante intenda creare una delega solamente per i servizi sanitari successivi]
    - Sola Consultazione
    - Completa
- il soggetto delegante comunica la sua scelta;
- l'operatore registra la volontà espressa dal delegante;
- l'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere al delegato, per Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina elencando tutte le scelte possibili e ricordando che è ammessa più di una scelta:
    - Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato;

Oppure, in alternativa alla delega di tipo "O":

Per l'accesso al Fascicolo Sanitario Elettronico (FSE):

- Delega di tipo "A": Accesso completo al FSE dell'assistito delegante con i massimi privilegi (accesso completo ai servizi, inclusi consultazione e inserimento dati);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme):

- Delega di tipo “B”: Consultazione dei dati e dei documenti relativi all’assistito presenti nel FSE;
- Delega di tipo “C”: Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché accesso alle informazioni sulle operazioni svolte sul proprio FSE (art. 21 Decreto del ministero Salute 7 settembre 2023);
- Delega di tipo “C-bis”: Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023);
- Delega di tipo “D”: Inserimento dei dati e documenti nel taccuino personale dell’assistito presente nel suo FSE.

Per l’accesso all’Ecosistema Dati sanitari (EDS):

- Delega di tipo “A- bis”: Accesso completo all’EDS dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-bis”: Consultazione dei dati e dei documenti relativi all’assistito presenti nel EDS;
- Delega di tipo “C-ter”: Accesso alla gestione dei consensi e le relative revoche dell’EDS;

Per l’accesso alla Piattaforma nazionale di Telemedicina (PNT):

- Delega di tipo “A- ter”: Accesso completo alla PNT dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-ter”: Consultazione dei dati e dei documenti relativi all’assistito presenti nella PNT;
- Delega di tipo “C-quater”: Accesso alla gestione dei consensi e le relative revoche della PNT;

- il soggetto delegante comunica la sua scelta;
- l’operatore registra opportunamente la volontà espressa dal delegante;
- i soggetti delegante e delegato forniscono opzionalmente i propri contatti telefonici o mail per la ricezione delle notifiche previste in merito l’utilizzo della delega;
- l’operatore chiede di inquadrare, fronte e retro, i documenti d’identità dei soggetti delegante e delegato, 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);
- l’operatore chiede di inquadrare, fronte e retro, la tessera sanitaria dei soggetti delegante e delegato, su cui è riportato il codice fiscale;
- l’operatore chiede ai soggetti di compiere una o più azioni casuali volte a rafforzare l’autenticità della richiesta;
- l’operatore riassume sinteticamente la volontà espressa dal soggetto delegante di conferire delega al soggetto delegato e raccoglie conferma dallo stesso.

ALLEGATO 3

“Modulo per la richiesta di registrazione della delega presentata dal delegante o, nei casi tassativamente previsti, dal delegato presso il Comune di residenza del delegante.”

Modulo per la richiesta di registrazione della delega presentata dal delegante o, nei casi tassativamente previsti[1], dal delegato presso il Comune di residenza del delegante (art. 5, commi 1 e 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGANTE> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

e-mail <EMAIL>

DELEGA

<NOME E COGNOME DEL DELEGATO> codice fiscale <CF>, nato/a il <DATA DI NASCITA DEL> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

e-mail <EMAIL>

AD EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL SOTTOSCRITTO AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

[1] Ai sensi dell'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, nel caso di cittadini allettati per lunga durata, ricoverati o impossibilitati per motivi sanitari a recarsi presso il Comune di residenza, la delega può essere presentata direttamente dal delegato.

La presente delega si intende (selezionare una delle opzioni seguenti):

- ☐ Nessun accesso **[selezionare nel caso si voglia creare solamente una delega per i servizi sanitari successivi]**
- ☐ Sola Consultazione
- ☐ Completa

Per l'accesso a Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma nazionale di Telemedicina del sottoscritto, la tipologia di delega conferita è la seguente (selezionare una o più tipologie tra quelle contemplate all'art. 11 del D.M. Salute del 7 settembre 2023 (FSE 2.0), a seconda dell'ambito di operatività della delega :

- ☐ **Tipo "0" [non delegato – se selezionato la delega generale creata per l'accesso ai servizi della pubblica amministrazione non è estesa ai servizi sanitari]**

OPPURE, in alternativa alla delega di Tipo "0"

Per l'accesso al Fascicolo Sanitario Elettronico (FSE), selezionare:

- ☐ **Tipo "A" [Accesso completo al FSE dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche)]**

Oppure, nel caso si vogliano selezionare solamente le singole funzioni senza i massimi privilegi, selezionare (anche insieme)

- ☐ Tipo "B" [Consultazione dei dati e dei documenti relativi all'assistito presenti nel FSE]
- ☐ Tipo "C" [Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché accesso alle informazioni sulle operazioni svolte sul proprio FSE (art. 21 Decreto del ministero Salute 7 settembre 2023]
- ☐ Tipo "C-bis" [Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)]
- ☐ Tipo "D" [Inserimento dei dati e documenti nel taccuino personale dell'assistito presente nel suo FSE]

Per l'accesso all'Ecosistema Dati sanitari (EDS), selezionare:

- ☐ **Tipo "A-bis" [Accesso completo all'EDS dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche)]**

Oppure, nel caso si vogliano selezionare solamente le singole funzioni senza i massimi privilegi, selezionare (in alternativa tra loro)

- ☐ Tipo "B-bis" [Accesso ai servizi e consultazione dei dati presenti nell'EDS, esclusa gestione dei consensi e relative revoche]
- ☐ Tipo "C-ter" [Accesso alla gestione dei consensi e le relative revoche dell'EDS]

Per l'accesso alla Piattaforma nazionale di Telemedicina (PNT), selezionare:

- ☐ **Tipo "A-ter" [Accesso completo alla PNT dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi)]**

Oppure, nel caso si vogliano selezionare solamente le singole funzioni senza i massimi privilegi, selezionare (in alternativa tra loro)

- ☐ Tipo "B-ter" [Accesso ai servizi e consultazione dei dati presenti nell'EDS, esclusa gestione dei consensi e relative revoche]
- ☐ Tipo "C-quater" [Accesso alla gestione dei consensi e le relative revoche della PNT]

Periodo di validità della delega[2]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca da parte del sottoscritto o rinuncia da parte del delegato.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del Delegante[3]

[2] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

[3] Apporre alla presenza dell'addetto al procedimento, fatta eccezione per le ipotesi di cui al citato art. 5, co.2.

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGANTE> codice fiscale <CF del delegante> - consapevole del fatto che le dichiarazioni mendaci, la falsità in atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. n. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del Delegante

Spazio riservato all'Ufficio.

(solo nel caso di delega presentata dal delegante ai sensi dell'art. 5, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe*)*

Le firme sono state apposte in mia presenza; ho identificato il sottoscrittore, che ha esibito un documento di riconoscimento in corso di validità.

Timbro e firma dell'addetto _

(solo nel caso di delega presentata dal delegato ai sensi dell'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe*)*

Attesto che la su esposta delega è stata presentata dal delegato ……. ……., che ho identificato previa esibizione di un documento di riconoscimento in corso di validità, il quale ha dichiarato che il delegante si trova in una condizione di impedimento temporaneo per ragioni di salute. La delega viene acquisita completa di copia del documento d'identità del delegante e di attestazione sanitaria.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note:

La delega deve essere sottoscritta dal delegante al momento della presentazione presso il Comune di residenza e alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità del delegante medesimo.

Solamente nei casi previsti all'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe (cittadini allettati per lunga durata, ricoverati o impossibilitati per motivi sanitari a recarsi presso il Comune di residenza) la delega potrà essere presentata dal delegato già sottoscritta dal delegante; in tal coso la delega dovrà essere corredata da:

1) copia del documento di identità del delegante;
2) copia di certificazione medica conforme all'allegato o certificazione rilasciata al delegante ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104.

Il delegato che presenta la delega dovrà in ogni caso esibire il proprio documento d'identità in corso di validità all'addetto al procedimento.

In riferimento all'art. 11, del D.M. Salute del 7 settembre 2023 (FSE 2.0), viene di seguito riportato il contenuto del comma *12:*

l'ambito di operatività della delega è ricompreso tra i seguenti:
a) accesso completo in base al quale il delegato opera sul FSE dell'assistito delegante con i medesimi privilegi (consultazione dei dati e dei documenti relativi all'assistito, inserimento di dati e documenti nel taccuino personale dell'assistito, nonché' accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché' oscuramenti e relative revoche);
oppure, singolarmente o in combinazione tra loro:

b) consultazione dei dati e dei documenti relativi all'assistito;
c) accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche;
d) inserimento di dati e documenti nel taccuino personale dell'assistito.

La delega può essere rilasciata a non più di due soggetti iscritti nell'ANPR (Anagrafe nazionale popolazione residente) ed è revocabile dal delegante in ogni momento tramite le funzionalità rese disponibili sul sito https://deleghedigitali.gov.it/ o recandosi presso il proprio Comune di residenza.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (art. 3, co.2 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal genitore esercente la responsabilità genitoriale o dal tutore presso il Comune di residenza del minore (art. 5, comma 6, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL GENITORE> codice fiscale <CF DEL GENITORE>, nato/a il <DATA NASCITA DEL GENITORE> a <LUOGO DI NASCITA DEL GENITORE>, documento d'identità n.ro <N.ro DOCUMENTO GENITORE> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL GENITORE>

RICHIEDE

la registrazione di una delega in qualità di esercente la responsabilità genitoriale sul minore <NOME E COGNOME DEL MINORE> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL MINORE AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

Periodo di validità della delega[4]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione per raggiungimento della maggiore età del minore.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del genitore o del tutore

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL GENITORE> codice fiscale <CF del genitore> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del genitore o del tutore

[4] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

Spazio riservato all'Ufficio.

Le firme sono stata apposte in mia presenza; ho identificato i sottoscrittori, che hanno esibito un documento di riconoscimento in corso di validità.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dall'esercente la responsabilità genitoriale o la tutela sul minore al momento della presentazione presso il Comune di residenza del minore medesimo.

È necessario esibire all'operatore un documento di riconoscimento in corso di validità.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal tutore, curatore o amministratore di sostegno presso il Comune di residenza del soggetto tutelato/inabilitato (art. 5, comma 6, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL TUTORE / CURATORE / AMMINISTRATORE DI SOSTEGNO> codice fiscale <CF>,

nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>,

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL>

RICHIEDE

la registrazione di una delega in qualità di TUTORE / CURATORE / AMMINISTRATORE DI SOSTEGNO di <NOME E COGNOME DEL TUTELATO/INABILITATO> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL TUTELATO/INABILITATO AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

Periodo di validità della delega[5]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione, per qualunque causa, della qualità di tutore/curatore/amministratore di sostegno.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del tutore / curatore / amministratore di sostegno

[5] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF del delegato> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n,. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del tutore / curatore / amministratore di sostegno

Spazio riservato all'Ufficio.

La firma è stata apposta in mia presenza; ho identificato il sottoscrittore che ha esibito un documento di riconoscimento.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dal tutore / curatore / amministratore di sostegno al momento della presentazione presso il Comune di residenza dell'interdetto/inabilitato/beneficiario alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal delegato presso il Comune di residenza del delegante (art. 5, comma 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF>,

nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>,

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL>

RICHIEDE

la registrazione di una delega in qualità di PROCURATORE di <NOME E COGNOME DEL SOGGETTO CHE HA CONFERITO LA PROCURA> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL RAPPRESENTATO…….. AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione, per qualunque causa, della qualità di procuratore.

Periodo di validità della delega[6]:

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del Delegato

DICHIARAZIONE LIBERATORIA

[6] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF del delegato> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n,. 445/2000, che la propria qualità di procuratore è tuttora sussistente e che non sono intervenute *medio tempore* modifiche o revoche.

Dichiara altresì, ai sensi del citato D.P.R. n. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del Delegato

Spazio riservato all'Ufficio.

La firma è stata apposta in mia presenza; ho identificato il sottoscrittore che ha esibito un documento di riconoscimento.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dal delegato al momento della presentazione presso il Comune di residenza dell'assistito alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità e di copia della procura notarile, generale o speciale, conferitagli

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

ALLEGATO 4

“Disciplinare tecnico”

DISCIPLINARE TECNICO

Caratteristiche tecniche e requisiti di sicurezza della piattaforma di gestione delle deleghe di cui all'articolo 64-ter del CAD

Definizioni

Si applicano le definizioni di cui al decreto cui questo allegato è parte integrante.

Introduzione

Il presente allegato definisce le caratteristiche tecniche e i requisiti di sicurezza della Piattaforma e le modalità operative per rendere disponibili la presentazione, accettazione e relativa registrazione della delega da parte dei cittadini iscritti nell'ANPR.

La Piattaforma è costituita dalle seguenti componenti:

a) Un'interfaccia web accessibile ai cittadini (Portale ai Cittadini);
b) Un'interfaccia web accessibile agli operatori comunali (Portale ai Comuni);
c) Un'interfaccia web accessibile agli operatori di backoffice (Portale di backoffice);
d) Un'interfaccia web accessibile agli operatori di helpdesk (Portale di helpdesk);
e) L'infrastruttura di backend della Piattaforma Deleghe (Backend).

1. 1 Portale ai Cittadini

La Piattaforma di Gestione Deleghe, mediante il "Portale ai cittadini", consente agli utenti autenticati di gestire in modo autonomo le deleghe digitali. Il "Portale Utente", in particolare, mette a disposizione degli utenti autenticati che intendono conferire una delega digitale (deleganti) le seguenti funzionalità:

- presentazione di una delega da parte del soggetto delegante;
- accettazione di una delega da parte del soggetto delegato;
- presentazione di una delega, da parte del soggetto delegato, ricevuta dal delegante tramite documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata e avanzata;
- presentazione di una delega in proprio favore da parte del soggetto delegato in qualità di esercente la responsabilità genitoriale o di tutore del minore;
- presentazione di una delega in proprio favore da parte del soggetto delegato in qualità di tutore, di curatore o di amministratore di sostegno del soggetto tutelato;
- presentazione di una delega in favore di soggetto terzo, presentata da parte del soggetto in qualità di esercente la responsabilità genitoriale, di tutore, di curatore o di amministratore di sostegno del soggetto tutelato o minore;
- richiesta di presentazione di una delega, da parte del soggetto delegato in videochiamata mediante il servizio di assistenza remota;
- revoca di una delega da parte del soggetto delegante;
- rinuncia di una delega da parte del soggetto delegato;
- visualizzazione delle deleghe inserite e relativi dettagli;
- visualizzazione delle richieste di utilizzo delle deleghe.

1.2. Portale ai Comuni

La Piattaforma di Gestione Deleghe, mediante il Portale rivolto ai Comuni, consente agli utenti autenticati addetti al procedimento di fruire delle seguenti funzionalità:

- inserimento di una delega presentata dal delegante, allegando copia su supporto informatico della documentazione presentata dallo stesso;

- inserimento di una delega presentata dal delegato procuratore, allegando copia della procura generale o speciale presentata dallo stesso;
- inserimento di una delega presentata dal delegato, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- inserimento della delega presentata dall'esercente la responsabilità genitoriale o tutore del minore, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- inserimento della delega presentata dal tutore, curatore dell'inabilitato e dall'amministratore di sostegno, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- revoca di una delega da parte del soggetto delegante.
- rinuncia di una delega da parte di un soggetto delegato

1.3. Portale di backoffice

La Piattaforma di Gestione Deleghe, mediante il Portale di backoffice, deve consentire agli operatori di back office autenticati di fruire delle seguenti funzionalità:

- verifica documentale e delle sottoscrizioni delle deleghe presentate dal delegato mediante il Portale rivolto ai cittadini e successiva registrazione della relativa delega;
- verifica dell'autocertificazione attestante la responsabilità resa dal genitore;
- registrazione di una delega mediante il servizio di assistenza remota in videochiamata;
- revoca di una delega, su richiesta del delegante;
- revoca di una delega, su ordine dell'Autorità giudiziaria trasmesso al Gestore della Piattaforma.

1.4. Portale di helpdesk

La Piattaforma di Gestione Deleghe, mediante il Portale di helpdesk, deve consentire agli operatori di helpdesk autenticati di fornire supporto a Comuni e cittadini.

1.5. Backend

La Piattaforma di Gestione Deleghe, mediante il Backend, deve consentire le seguenti funzionalità:

- verifica dell'iscrizione in ANPR del delegante e del delegato mediante cooperazione con il sistema ANPR attraverso PDND;
- verifica della qualità di esercente la responsabilità genitoriale mediante cooperazione con il Ministero della Giustizia attraverso PDND.
- verifica della qualità di tutore, di curatore o di amministratore di sostegno mediante cooperazione con il Ministero della Giustizia attraverso PDND;
- verifica del possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 attraverso PDND;
- verifica dell'elenco dei soggetti deceduti per il blocco delle deleghe attive;
- verifica della decadenza o sospensione della responsabilità genitoriale o dell'avvenuta emancipazione del minore per il blocco delle deleghe attive;
- verifica della decadenza o sospensione della qualità di tutore, di curatore o di amministratore di sostegno, per il blocco delle deleghe attive;
- verifica di validità temporale della delega;
- verifica che non siano presenti più di due deleghe per delegante.
- verifica del numero massimo di 5 deleghe per soggetto delegato, escluso i casi di esercente responsabilità genitoriale e tutori, curatori o amministratori di sostegno nonché dai procuratori generali e speciali.

- La delega può essere nuovamente presentata anche prima della scadenza; in tale caso, il termine della durata di cui al comma 1, decorre dalla data della nuova presentazione e dalla medesima data, la delega precedente si intende sostituita.

2. Integrazione con basi dati nazionali

La Piattaforma di Gestione Deleghe abilita l'interoperabilità con i sistemi informativi e le banche dati nazionali al fine gestire le deleghe digitali.

L'interoperabilità con i sistemi informativi e le banche dati nazionali è volta all'implementazione delle seguenti verifiche e funzionalità:

- **Verifica dei soggetti deceduti:**
  La Piattaforma coopera con i servizi del sistema ANPR, tramite la PDND, al fine di procedere al blocco delle deleghe attive riferite a soggetti deceduti. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per tali soggetti.
- **Verifica dell'iscrizione in ANPR dei soggetti deleganti e delegati:**
  La Piattaforma coopera con i servizi del sistema ANPR, tramite la PDND, anche al fine di assicurare l'allineamento delle informazioni anagrafiche ai sensi dell'articolo 62, comma 5, del CAD quali, in particolare, quelle relative all'iscrizione del cittadino delegante e delegato nell'ANPR, all'identificativo univoco del cittadino (ID ANPR), al numero e data di scadenza della carta di identità e al domicilio digitale del cittadino ove presente.
- **Verifica di sussistenza della qualità di esercente la responsabilità genitoriale:**
  La Piattaforma coopera con i servizi del Ministero della Giustizia tramite la PDND, per le verifiche di sussistenza della qualità di esercente la responsabilità genitoriale. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata in favore di tali soggetti. In assenza dei suddetti servizi verranno utilizzati i servizi di verifica di maternità, paternità e stato di famiglia esposti da ANPR attraverso PDND.
- **Verifica di sussistenza della qualità di tutore, di curatore o di amministratore di sostegno:**
  La Piattaforma coopera con i servizi del Ministero della Giustizia, tramite la PDND, al fine di ricevere giornalmente i dati afferenti alle nuove nomine o variazioni della qualifica di tutore, di curatore o di amministratore di sostegno e dell'assenza di provvedimenti di sospensione o ablativi della responsabilità genitoriale, procedendo al blocco tempestivo delle deleghe attive. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per tali soggetti.
- **Verifica del possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104**:
  La Piattaforma coopera con i servizi dell'INPS, tramite la PDND, al fine di appurare il possesso, da parte del delegante, del requisito necessario per richiedere la creazione della delega tramite Assistenza Remota. Tali dati sono conservati per il tempo strettamente necessario a finalizzare la richiesta di appuntamento.

3. Servizi per la richiesta e il rilascio della delega

La richiesta di accesso ai servizi ai cittadini descritti dal presente decreto è possibile dall'area dedicata della piattaforma di gestione deleghe previa identificazione mediante le modalità di cui ai commi 2-quater e 2-nonies dell'art. 64 del CAD.

3.1 Creazione della delega

Un cittadino delegante richiede una delega a favore di un altro cittadino tramite "Portale ai Cittadini" (Art. 3, comma 2.a)

1. Il cittadino delegante accede al Portale e avvia la richiesta di delega;
2. Il Portale ai Cittadini verifica che il cittadino (delegante e delegato) sia iscritto su ANPR;
3. Il Portale ai Cittadini deve richiedere al delegante di effettuare le seguenti scelte:
    - selezionare, per la delega generale, se quest'ultima deve essere:
        - Nessun accesso [l'opzione è disponibile nel caso in cui il delegante intenda creare una delega solamente per i servizi sanitari successivi]
        - Sola consultazione
        - Completa
    - selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
    - Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato;

Oppure, in alternativa alla delega di tipo "O":

Per l'accesso ai servizi del FSE

- Delega di tipo "A": Accesso completo al FSE dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme)

- Delega di tipo "B": Consultazione dei dati e dei documenti relativi all'assistito presenti nel FSE;

- Delega di tipo "C": Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché l'ulteriore diritto di accesso alle informazioni relative alle operazioni di cui all'art. 21 del decreto del 7 settembre 2023, come previsto dall'art. 9, comma 1, del medesimo decreto;

- Delega di tipo "C-bis": Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)

- Delega di tipo "D": Inserimento dei dati e documenti nel taccuino personale dell'assistito presente nel suo FSE.

Per l'accesso ai servizi EDS

- Delega di tipo “A-bis”: Accesso completo all’EDS dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-bis”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nel EDS (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-ter”: Accesso alla gestione dei consensi e le relative revoche dell’EDS;

Per l'accesso ai servizi PNT

- Delega di tipo “A-ter”: Accesso completo alla PNT dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-ter”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nella PNT (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-quater”: Accesso alla gestione dei consensi e le relative revoche della PNT;

4. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega entro trenta giorni, confermando che agisce a titolo personale, senza finalità professionali o economiche (art.8, comma 2);
5. Il Portale registra la delega richiesta e accettata dal delegato.
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega.

<u>Un cittadino delegato registra una delega per conto di un altro cittadino tramite Portale ai Cittadini (Art. 3, comma 2.b)</u>

1. Il cittadino delegante compila e sottoscrive, con firma digitale o altro tipo di firma elettronica qualificata o avanzata (realizzata ai sensi dell’articolo 16 del decreto del ministero dell’Interno 8 settembre 2022), il modulo fornito dal Portale e lo consegna al delegato in formato digitale;
2. Il cittadino delegato accede al Portale e carica i documenti forniti dal delegante confermando che agisce a titolo personale, senza finalità professionali o economiche (art.8, comma 2)
3. Il Portale Deleghe verifica che il cittadino (delegante e delegato) sia iscritto su ANPR;
4. Il Portale ai Cittadini deve richiedere al delegato di effettuare le seguenti scelte:
   4.1. selezionare, per la delega generale, se quest’ultima deve essere:
   - Nessun accesso [l’opzione è disponibile nel caso in cui il delegante intenda creare una delega solamente per i servizi sanitari successivi]
   - Sola consultazione
   - Completa

   4.2. selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
   - Delega di tipo “0” (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall’operatività del delegato;

Oppure, in alternativa alla delega di tipo “O”:

Per l'accesso ai servizi del FSE

- Delega di tipo “A”: Accesso completo al FSE dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme)

- Delega di tipo “B”: Consultazione dei dati e dei documenti relativi all’assistito presenti nel FSE;
- Delega di tipo “C”: Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché l’ulteriore diritto di accesso alle informazioni relative alle operazioni di cui all'art. 21 del decreto del 7 settembre 2023, come previsto dall’art. 9, comma 1, del medesimo decreto;
- Delega di tipo “C-bis”: Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)
- Delega di tipo “D”: Inserimento dei dati e documenti nel taccuino personale dell’assistito presente nel suo FSE.

Per l'accesso ai servizi EDS

- Delega di tipo “A-bis”: Accesso completo all’EDS dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-bis”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nel EDS (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-ter”: Accesso alla gestione dei consensi e le relative revoche dell’EDS;

Per l'accesso ai servizi PNT

- Delega di tipo “A-ter”: Accesso completo alla PNT dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo “B-ter”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nella PNT (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-quater”: Accesso alla gestione dei consensi e le relative revoche della PNT;

Un cittadino esercente la responsabilità genitoriale registra una delega per un minore tramite Portale ai Cittadini (Art. 3, comma 2.c)

1. Il cittadino esercente la responsabilità genitoriale verso un minore accede al Portale e fa richiesta di registrazione della relativa delega;
2. Il Portale verifica il legame di filiazione e l'emancipazione del minore interrogando i servizi di ANPR;
3. Il Portale verifica che il cittadino esercente la responsabilità genitoriale e il minore siano iscritti su ANPR;
4. Il Portale verifica le informazioni tramite PDND nel dominio Giustizia;
5. Il Portale registra la delega richiesta dal cittadino in quanto esercente la responsabilità genitoriale;

Nelle more della disponibilità dei servizi del Ministero di Giustizia:

1. Il cittadino accede al Portale Cittadini, dove prima di registrare la delega dichiara, ai sensi del DPR 445/2000 e s.m.i., la propria qualità di esercente la responsabilità genitoriale sul minore;
2. Il Portale verifica tramite i servizi di ANPR in PDND che il cittadino e il minore siano iscritti su ANPR;
3. Il Portale verifica tramite i servizi di ANPR in PDND il legame di genitorialità;
4. Il Portale verifica tramite i servizi di ANPR in PDND l'emancipazione del minore tramite l'accertamento di matrimonio;
5. Il Portale registra la delega richiesta dal cittadino in quanto esercente la responsabilità genitoriale.

Quando la delega è presentata dagli esercenti la responsabilità genitoriale si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo "A", "A-bis" e "A-ter".

Un cittadino tutore, curatore dell'inabilitato e amministratore di sostegno registra una delega ad operare per conto del tutelato, dell'inabilitato e beneficiario dell'amministrazione di sostegno tramite Portale ai Cittadini (Art. 3, comma 2.d)

1. Il cittadino tutore, curatore o amministratore di sostegno di un altro cittadino accede al Portale e registra la relativa delega;
2. Il Portale verifica che il cittadino tutore, curatore o amministratore di sostegno e il tutelato siano iscritti su ANPR;
3. Il Portale verifica le informazioni tramite PDND nel dominio Giustizia;
4. Il Portale registra la delega richiesta dal cittadino in quanto tutore, curatore o amministratore di sostegno.

Quando la delega è presentata da tutori, curatori, amministratori di sostegno nonché dai procuratori generali si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo "A", "A-bis" e "A-ter".

Un cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell'inabilitato e l'amministratore di sostegno registra una delega per operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno in favore di un altro soggetto (Art. 3, comma 2.e)

1. Il cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell'inabilitato o l'amministratore di sostegno accede al Portale e presenta la delega ad operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno in favore di un altro soggetto;
2. Il Portale Deleghe verifica che le parti coinvolte (minore/interdetto/inabilitato, delegante, delegato) siano iscritti in ANPR;
3. Il Portale ai Cittadini deve richiedere al delegante di effettuare le seguenti scelte:
    3.1. selezionare, per la delega generale, se quest'ultima deve essere:
        - Nessun accesso [l'opzione è disponibile nel caso in cui il delegante intenda creare una delega solamente per i servizi sanitari successivi]
        - Sola consultazione
        - Completa
    3.2. selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
    - Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato;

Oppure, in alternativa alla delega di tipo "O":

Per l'accesso ai servizi del FSE

- Delega di tipo "A": Accesso completo al FSE dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme)

- Delega di tipo "B": Consultazione dei dati e dei documenti relativi all'assistito presenti nel FSE;

- Delega di tipo "C": Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché l'ulteriore diritto di accesso alle informazioni relative alle operazioni di cui all'art. 21 del decreto del 7 settembre 2023, come previsto dall'art. 9, comma 1, del medesimo decreto;

- Delega di tipo "C-bis": Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)

- Delega di tipo "D": Inserimento dei dati e documenti nel taccuino personale dell'assistito presente nel suo FSE.

Per l'accesso ai servizi EDS

- Delega di tipo "A-bis": Accesso completo all'EDS dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo "B-bis": Accesso ai servizi e consultazione dei dati relativi all'assistito presenti nel EDS (esclusa gestione dei consensi e relative revoche);
- Delega di tipo "C-ter": Accesso alla gestione dei consensi e le relative revoche dell'EDS;

Per l'accesso ai servizi PNT

- Delega di tipo "A-ter": Accesso completo alla PNT dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo "B-ter": Accesso ai servizi e consultazione dei dati relativi all'assistito presenti nella PNT (esclusa gestione dei consensi e relative revoche);
- Delega di tipo "C-quater": Accesso alla gestione dei consensi e le relative revoche della PNT;

4. Il Portale Deleghe verifica le informazioni tramite PDND nel dominio Giustizia;
5. Il Portale registra la delega all'accettazione del delegato.
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega.

<u>Presentazione della delega con l'assistenza remota (web meeting) del Gestore della Piattaforma (Art. 4)</u>

1. Il cittadino delegante (di età pari o superiore ai 65 anni o in possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104) fornisce copia del proprio documento d'identità, il codice fiscale e dichiarazione relativa al possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 (se applicabile);
2. Il cittadino delegato:
   2.1. accede al Portale mediante l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo;
   2.2. carica sul Portale i documenti forniti dal delegante, la copia della propria carta d'identità e la copia del proprio codice fiscale.
3. La piattaforma verifica:
   3.1. che il delegante ed il delegato siano iscritti in ANPR;
   3.2. il possesso dei requisiti per l'erogazione del servizio da parte del delegante; per la verifica del possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 il Gestore verifica i relativi servizi INPS mediante PDND;
4. All'esito positivo delle sopracitate verifiche, Il cittadino delegato richiede un appuntamento per l'erogazione del servizio, selezionando una tra le date e gli orari disponibili;
5. L'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere, in generale, al delegato elencando le due opzioni di scelta possibili:
   - Nessun accesso [l'opzione è disponibile nel caso in cui il delegante intenda creare una delega solamente per i servizi sanitari successivi]

- Sola Consultazione
- Completa

6. Il soggetto delegante comunica la sua scelta;
7. L'operatore registra la volontà espressa dal delegante;
8. L'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere al delegato, per Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina elencando tutte le scelte possibili e ricordando che è ammessa più di una scelta:
    - Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato;

Oppure, in alternativa alla delega di tipo "O":

Per l'accesso ai servizi del FSE

- Delega di tipo "A": Accesso completo al FSE dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme)

- Delega di tipo "B": Consultazione dei dati e dei documenti relativi all'assistito presenti nel FSE;
- Delega di tipo "C": Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché l'ulteriore diritto di accesso alle informazioni relative alle operazioni di cui all'art. 21 del decreto del 7 settembre 2023, come previsto dall'art. 9, comma 1, del medesimo decreto;
- Delega di tipo "C-bis": Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)
- Delega di tipo "D": Inserimento dei dati e documenti nel taccuino personale dell'assistito presente nel suo FSE.

Per l'accesso ai servizi EDS

- Delega di tipo "A-bis": Accesso completo all'EDS dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo "B-bis": Accesso ai servizi e consultazione dei dati relativi all'assistito presenti nel EDS (esclusa gestione dei consensi e relative revoche);
- Delega di tipo "C-ter": Accesso alla gestione dei consensi e le relative revoche dell'EDS;

Per l'accesso ai servizi PNT

- Delega di tipo "A-ter": Accesso completo alla PNT dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);

Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):

- Delega di tipo "B-ter": Accesso ai servizi e consultazione dei dati relativi all'assistito presenti nella PNT (esclusa gestione dei consensi e relative revoche);
- Delega di tipo "C-quater": Accesso alla gestione dei consensi e le relative revoche della PNT;

9. Il soggetto delegante comunica la sua scelta;
10. L'operatore registra opportunamente la volontà espressa dal delegante;
11. La delega è registrata sul Portale a seguito della conclusione con esito positivo dell'erogazione del servizio di web meeting;
12. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Ulteriori dettagli riportati in Allegato 1.

<u>Un cittadino delegante presenta una delega a favore di un altro soggetto tramite sportello presso il proprio comune di residenza (Art. 5, comma 1)</u>

1. Il cittadino delegante presenta allo sportello comunale il modulo delega;
2. L'impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
4. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega;
5. Il Portale registra la delega all'accettazione del delegato;
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

<u>Un cittadino delegato in possesso di una procura generale o speciale richiede una delega tramite lo sportello presso il comune di residenza del delegante (Art. 5, comma 1)</u>

1. Un cittadino delegato esibisce allo sportello comunale copia della procura generale o speciale copia del proprio documento di identità;
2. L'impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
4. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Quando la delega è presentata dai procuratori generali si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo "A", "A-bis" e "A-ter".

<u>Un cittadino delegato presenta una delega in proprio favore tramite sportello presso il comune di residenza del delegante (Art. 5, comma 2)</u>

1. Il cittadino delegante consegna al delegato il modulo delega firmato e il certificato medico;
2. Il cittadino delegato presenta allo sportello comunale il modulo delega e il certificato medico;
3. L'impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
4. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
5. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega;
6. Il Portale registra la delega all'accettazione del delegato;

7. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Un cittadino esercente la responsabilità genitoriale, tutore, curatore dell'inabilitato e amministratore di sostegno presenta una delega per operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno tramite sportello presso il comune di residenza (Art. 5, comma 6)

1. Il cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell'inabilitato o l'amministratore di sostegno presenta allo sportello comunale il modulo delega;
2. L'impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale Deleghe verifica le informazioni tramite PDND nel dominio Giustizia;
4. Il Portale registra la delega;
5. Il cittadino delegato riceve la notifica di registrazione della delega.

3.2 Utilizzo della delega

In fase di accesso da parte del delegato ai servizi in rete erogati dalle Pubbliche Amministrazioni che richiedono l'identificazione informatica, il Gestore dell'identità digitale (IdP) abilita la possibilità per il cittadino di scegliere se operare per conto di un soggetto delegante.
Nel caso in cui il cittadino scelga di operare per conto di un soggetto delegante l'IdP interroga la Piattaforma per verificare la sussistenza di una delega valida.
Se la risposta della Piattaforma è positiva, l'IdP consente l'accesso al delegato per conto del delegante ed invia al SP l'informazione che l'accesso avviene mediante delega.
L'IdP, inoltre, deve trasferire al SP l'informazione se la delega è Nessun accesso, in Sola consultazione o Completa e nei soli casi in cui il SP gestisca il Fascicolo Sanitario Elettronico, l'Ecosistema Dati Sanitari, la Piattaforma Nazionale di Telemedicina l'IdP deve trasferire anche l'informazione relativa al tipo di delega concesso (0/A/A-bis/A-ter/B/B-bis/B-ter/C/C-bis/C-ter/C-quater/D).

Utilizzo della delega

Di seguito si dettagliano gli step necessari all'utilizzo della delega.

1. Il cittadino accede ad un servizio in rete erogato da una Pubblica Amministrazione (SP);
2. Il cittadino in fase di autenticazione esprime la volontà di operare come delegato;
3. L'IdP, su richiesta del cittadino delegato, effettuata il reindirizzamento su una pagina della Piattaforma;
4. La Piattaforma, con opportune misure di sicurezza, recupera le deleghe conferite al delegato, effettua le verifiche di validità previste (quali l'esistenza in vita del delegante, la verifica di sussistenza della qualità di esercente la responsabilità genitoriale o la verifica di sussistenza della qualità di tutore, di curatore o di amministratore di sostegno) e mostra l'elenco delle deleghe valide all'utente;
5. Il delegato seleziona la delega, esprime il consenso ad inviare all'IdP i dati necessari all'accesso mediante delega;
6. Il cittadino delegante, laddove previsto dal DPCM, riceve una notifica di richiesta di utilizzo della delega da parte del delegato;
7. L'IdP riceve dalla Piattaforma i dati necessari o restituisce un errore nei casi previsti;
8. L'IdP presenta i dati del delegante, sostituiti a quelli del delegato, in fase di autenticazione al servizio erogato dal SP.

3.3 Revoca e rinuncia della delega

Il delegante può in ogni momento revocare la delega tramite le funzionalità rese disponibili dal Portale o recandosi presso il proprio comune di residenza.
Il delegato può rinunciare in qualsiasi momento alle deleghe precedentemente accettate utilizzando una specifica funzionalità resa disponibile nel Portale.
La delega è revocata automaticamente nel caso di esito negativo delle seguenti verifiche:

- Sussistenza delle qualità di esercente la responsabilità genitoriale (dato del Ministero Giustizia) o emancipazione del minore (dato presente in ANPR);
- Sussistenza delle qualità di tutore, di curatore o di amministratore di sostegno (dato del Ministero Giustizia);
- Decesso del delegante/delegato (Servizio di "esistenza in vita" di ANPR).

La delega viene inoltre revocata su richiesta dell'Autorità Giudiziaria.

4. Misure di sicurezza

Il presente paragrafo elenca le misure di sicurezza tecniche e organizzative messe in atto dal Gestore della piattaforma.

Le misure di sicurezza sono individuate nel rispetto delle disposizioni in materia di cybersicurezza e, in particolare, di quelle previste dalla legge 28 giugno 2024, n. 90, e dal regolamento di cui al decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 27 giugno 2024, n. 21007.

Le misure di sicurezza sono organizzate nelle funzioni, categorie e sottocategorie del "Framework nazionale per la cybersecurity e la data protection", edizione 2019.

Per ogni misura è fornito un elenco di punti che rappresentano i requisiti dell'implementazione minima attesa.

Il termine "soggetto", ovunque ricorra nel presente paragrafo, è da intendersi riferito al Gestore della piattaforma.

Ad eccezione dell'organizzazione di cybersecurity (definita alla misura ID.AM-6), il termine "organizzazione", ovunque ricorra nel presente paragrafo, è da intendersi riferito almeno ai sistemi informativi e di rete tramite i quali è realizzata la piattaforma, nonché alle strutture e al personale del Gestore della piattaforma a vario titolo coinvolti nell'ambito dello sviluppo e della gestione della piattaforma.

4.1 Identificazione

4.1.1 Gestione degli asset (Asset Management) (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facility necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.

4.1.1.1 ID.AM-1. Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione.

1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. L'accesso alla rete è consentito esclusivamente ai soli sistemi e apparati fisici approvati.

4.1.1.2 ID.AM-2. Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione.

1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.

2. L'installazione è consentita esclusivamente alle piattaforme e applicazioni software approvate.

4.1.1.3 ID.AM-3. I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati.

1. Tutti i flussi informativi tra i sistemi informativi e di rete dell'organizzazione e l'esterno sono identificati ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. Le comunicazioni sono consentite esclusivamente per i flussi informativi approvati.

4.1.1.4 ID.AM-6. Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).

1. È definita e resa nota alle articolazioni del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. All'interno dell'organizzazione di cui al punto 1, è istituita e resa nota alle articolazioni del soggetto la struttura responsabile per l'attuazione delle misure di sicurezza di cui al presente allegato.
3. Esiste un elenco del personale interno ed esterno dell'organizzazione di cui al punto 1, ivi incluso quello della struttura di cui al punto 2, avente specifici ruoli e responsabilità.

4.1.2 Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.

4.1.2.1 ID.GV-1. È identificata e resa nota una policy di cybersecurity.

1. Le politiche e i processi di cybersecurity sono definiti per almeno i seguenti ambiti:
   a) governo;
   b) gestione del rischio;
   c) gestione degli asset;
   d) gestione del rischio di cybersecurity della catena di approvvigionamento;
   e) gestione delle vulnerabilità;
   f) business continuity e disaster recovery;
   g) gestione delle identità digitali, autenticazione e controllo degli accessi;
   h) sicurezza dei dati;
   i) manutenzione e riparazione dei sistemi;
   j) protezione delle reti;
   k) monitoraggio degli eventi di sicurezza;
   l) risposta e ripristino agli incidenti;
   m) formazione del personale.
2. Esiste un documento aggiornato che descrive le politiche di cybersecurity di cui al punto 1.
3. Esiste un documento aggiornato che descrive i processi di cybersecurity di cui al punto 1.
4. Le politiche e i processi di cui al punto 1 sono revisionati periodicamente e quando necessario.

4.1.2.2 ID.GV-4. La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.

1. Esiste un piano aggiornato per la gestione del rischio informatico.

4.1.3 Valutazione del rischio (Risk Assessment) (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.

4.1.3.1 ID.RA-1. Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, esiste un piano aggiornato che descrive l'insieme delle attività finalizzate all'identificazione delle vulnerabilità contenente almeno:
    a) le modalità per l'identificazione delle vulnerabilità;
    b) la pianificazione delle attività per l'identificazione delle vulnerabilità.
2. Sono eseguite periodicamente le attività per identificare le vulnerabilità di cui al punto 1 e predisposte apposite relazioni che contengono almeno:
    a) la descrizione generale delle attività effettuate e gli esiti delle stesse;
    b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza.

4.1.3.2 ID.RA-5. Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.

1. In accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4, esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno:
    a) l'identificazione del rischio;
    b) l'analisi del rischio;
    c) la ponderazione del rischio.
2. La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti.

4.1.3.3 ID.RA-6. Sono identificate e prioritizzate le risposte al rischio.

1. Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità.
2. Per il rischio residuo successivo al trattamento di cui al punto precedente, esiste un documento aggiornato che ne contiene la chiara descrizione. Il documento, con il quale si accetta il rischio residuo, è approvato da parte dei vertici del soggetto.

4.1.4 Gestione del rischio relativo alla catena di approvvigionamento (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

4.1.4.1 ID.SC-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione

1. Esiste un documento aggiornato di dettaglio, che descrive i processi di gestione del rischio inerente alla catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

4.1.4.2 ID.SC-2. I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber.

1. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi di information and communication technology (ICT).

4.1.4.3 ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber

1. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, con le misure di sicurezza applicate ai sistemi informativi e di rete della piattaforma. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.
2. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, con le misure di sicurezza applicate ai sistemi informativi e di rete della piattaforma. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.

4.1.4.4 ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1. Esiste un documento aggiornato recante, almeno, le modalità e la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.
2. Esiste una pianificazione aggiornata degli audit, verifiche, o altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.

4.2 Protezione

4.2.1 Gestione delle identità, autenticazione e controllo degli accessi (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

4.2.1.1 PR.AC-1. Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.

1. Salvo motivate e documentate ragioni di natura organizzativa o tecnica, le identità digitali sono individuali per gli utenti.
2. Le credenziali di accesso relative alle identità digitali sono robuste e aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
3. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono verificate periodicamente le identità digitali e le credenziali di accesso, aggiornandole/revocandole in caso di variazioni (es. trasferimento o cessazione di personale).
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
6. In relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV 1.

4.2.1.2 PR.AC-3. L'accesso remoto alle risorse è amministrato.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono monitorati gli accessi da remoto ed esiste un log degli accessi da remoto eseguiti.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono definite le attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.

4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alla gestione degli accessi da remoto, esiste un documento aggiornato contenente almeno:
   a) l'elenco dei sistemi informativi e di rete ai quali è possibile accedere e le relative modalità;
   b) le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.1.3 PR.AC-4. I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

1. Le identità digitali sono assegnate in accordo al principio del privilegio minimo e nel rispetto del principio di separazione delle funzioni.
2. È assicurata la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.
3. Tutte le utenze con privilegi sono censite, approvate e utilizzate quando necessario registrando ogni accesso effettuato.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3
6. In relazione alla gestione dei diritti di accesso e alle relative autorizzazioni, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.1.4 PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)

1. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla misura ID.RA-5, contiene almeno:
   a) le modalità di autenticazione disponibili;
   b) la loro assegnazione alle categorie di transazioni.
2. La piattaforma consente l'accesso al delegante/delegato esclusivamente mediante un'autenticazione basata sull'identità digitale CIE e/o SPID con livello di sicurezza almeno significativo.

4.2.2 Consapevolezza e addestramento (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti

4.2.2.1 PR.AT-1. Tutti gli utenti sono informati e addestrati.

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita al personale dell'organizzazione e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco del personale che ha ricevuto la formazione e i relativi contenuti.

4.2.2.2 PR.AT-2. Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti.

4.2.3 Sicurezza dei dati (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.

4.2.3.1 PR.DS-1. I dati memorizzati sono protetti.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, salvo motivate e documentate ragioni di natura organizzativa o tecnica, sono utilizzati sistemi di cifratura dei dati, ivi compresi i dispositivi portatili e quelli removibili.
2. Sono impiegate tecniche di pseudonimizzazione dei dati personali.
3. Gli algoritmi e i parametri di cifratura e delle tecniche di pseudonimizzazione sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
6. In relazione alla memorizzazione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.3.2 PR.DS-2: I dati sono protetti durante la trasmissione

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, salvo motivate e documentate ragioni di natura organizzativa o tecnica, le comunicazioni, inclusi i flussi di cui alla misura ID.AM-3, sono cifrati con protocolli e algoritmi allo stato dell'arte.
2. Gli algoritmi e i parametri di cifratura delle comunicazioni sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
5. In relazione alla trasmissione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.3.3 PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni.

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
    a) l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni;
    b) le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;
    c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

2. I meccanismi di controllo dell'integrità dei dati di cui al punto 1, lettera a) sono conformi alle Linee guida funzioni crittografiche emanate da ACN.

4.2.3.4 PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione.

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
    a) l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata;
    b) le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione;
    c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4.2.4 Procedure e processi per la protezione delle informazioni (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset.

4.2.4.1 PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)

1. Sono definite, e documentate in un elenco, le configurazioni di riferimento sicure (*hardened*) per i sistemi IT.
2. Salvo motivate e documentate ragioni di natura organizzativa o tecnica, sono consentiti l'installazione e l'utilizzo delle sole configurazioni di cui al punto 1.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alle configurazioni di riferimento dei sistemi IT, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.4.2 PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).

1. La piattaforma è sviluppata secondo le linee guida di sicurezza nello sviluppo delle applicazioni dell'Agenzia per l'Italia Digitale e le migliori pratiche di riferimento.
2. Viene gestito il ciclo di vita della piattaforma e dei relativi sistemi informativi e di rete.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 2.

4.2.4.3 PR.IP-4. I backup delle informazioni sono eseguiti, amministrati e verificati.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono effettuati periodicamente i backup dei dati.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è assicurata la riservatezza delle informazioni contenute nei backup mediante cifratura.

3. Gli algoritmi e i parametri di cifratura impiegati per assicurare la riservatezza delle informazioni contenute nei backup di cui al punto 2 sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
4. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.
5. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
6. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
7. In relazione al backup dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.4.4 PR.IP-9. Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.

1. Esistono piani aggiornati di continuità operativa/disaster recovery redatti in accordo alle relative politiche e ai relativi processi di cui alla misura ID.GV-1.

4.2.4.5 PR.IP-12. Viene sviluppato e implementato un piano di gestione delle vulnerabilità.

1. Le vulnerabilità emerse a seguito delle attività di cui al punto 2 della misura ID.RA-1 sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero, se del caso, accentando il rischio in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla gestione delle vulnerabilità, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.5 Manutenzione (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.

4.2.5.1 PR.MA-1. La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5:
    a) i sistemi informativi e di rete sono aggiornati all'ultima versione raccomandata dal produttore;
    b) l'aggiornamento dei software, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.

4. In relazione alla manutenzione e riparazione dei sistemi informativi e di rete, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.5.2 PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.
2. Tutti gli accessi eseguiti da remoto da personale di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.
3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, devono essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
6. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2, 3, 4 e 5.
7. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2, 3, 4 e 5.
8. In relazione alla manutenzione delle risorse e dei sistemi svolta da remoto, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.6 Tecnologie per la protezione (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

4.2.6.1 PR.PT-1. Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla conservazione dei log, con particolare riguardo all'integrità e alla disponibilità degli stessi, esiste un documento aggiornato contenente almeno le procedure, le metodologie e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.
5. **È registrata la motivazione dell'accesso ai log**

4.2.6.2 PR.PT-4. Le reti di comunicazione e controllo sono protette.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati i sistemi perimetrali, quali firewall, anche a livello applicativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.

3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1
4. In relazione alla protezione delle reti, esiste un documento aggiornato contenente almeno le procedure e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.3 Rilevamento

4.3.1 Monitoraggio continuo per la sicurezza (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

4.3.1.1 DE.CM-1. Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati sistemi di rilevamento delle intrusioni (intrusion detection systems - IDS).
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è monitorato il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali al fine di rilevare gli eventi di cybersecurity.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione al monitoraggio degli eventi di sicurezza, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.3.1.2 DE.CM-4. Il codice malevolo viene rilevato.

1. Sono presenti e aggiornati sistemi di protezione delle postazioni terminali.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.).
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. Esiste un documento aggiornato contenente almeno le procedure, le metodologie e le tecnologie impiegate per il rispetto delle politiche di cui al punto 3 e nell'ambito dei processi di cui al punto 4.

4.3.1.3 DE.CM-8. Vengono svolte scansioni per l'identificazione di vulnerabilità

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment prima della loro messa in esercizio.
2. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software.
3. Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.

4. Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.
5. Nell'ambito dei punti 1 e 2 è inclusa l'esecuzione di *Web application penetration test* (WAPT), per la verifica della presenza di eventuali vulnerabilità sul codice sorgente.
6. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2, 3, 4 e 5.
7. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2, 3, 4 e 5.
8. Esiste un documento aggiornato contenente almeno le procedure, le metodologie e le tecnologie impiegate per il rispetto delle politiche di cui al punto 6 e nell'ambito dei processi di cui al punto 7.

4.4 Risposta

4.4.1 Pianificazione della risposta (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

4.4.1.1.RS.RP-1. Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente.

1. Esiste un piano aggiornato di risposta agli incidenti all'interno del quale sono definiti almeno:

f) le articolazioni preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche;
g) le procedure per la notifica degli incidenti alle parti interessate;
h) le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.4.2 Analisi (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.

4.4.2.1 RS.AN-5. Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza).

1. In relazione alla gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia, nonché da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento, esiste un documento aggiornato contenente almeno:

i) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni;
j) le procedure, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui alla lettera a) nel rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV1.

4.5 Recupero

4.5.1 Pianificazione del ripristino (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

4.5.1.1 RC.RP-1. Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.

1. Esiste un piano di ripristino che prevede almeno, le procedure necessarie al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da un incidente di cybersecurity.

5. Accessibilità

La “Piattaforma di Gestione Deleghe” rispetta i criteri di accessibilità di cui alla legge 9 gennaio 2004, n. 4, nel rispetto dei principi di usabilità, completezza di informazione, chiarezza del linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità e interoperabilità.

ALLEGATO 5

“Profilo implementativo per il protocollo di utilizzo di una delega”

Dettaglio versione

Versione	Data	Modifiche	Autore
1.0	02/02/2026	Prima versione	IPZS
2.0	30/09/2026	-Recepimento delle modifiche sugli accessi all'ambito sanitario: introduzione dell'opzione "Nessun accesso" (che si traduce nell'accesso al solo ambito sanitario); ridefinizione della delega FSE/EDS/PNT di tipo “B”, "C" e “D”, introduzione dei tipi “A-bis”, “A-ter”, "B-bis", "B-ter", "C-bis", “C-ter” e “C-quater”. - Correzione formato richiesta Token Endpoint, specifica del flusso di onboarding di un IdP, gestione del materiale crittografico e offboarding di un IdP. Modificato il nome del campo “contact” in “email”. Corretti esempi non normativi. Chiarimenti sulla costruzione del parametro claims nel PAR Endpoint. -Aggiornamento richiesta PAR, servizi PGD-SP e PGD-IdP e esempi non normativi. - Chiarimenti sul ruolo privacy degli IdP e integrazione delle informazioni privacy nel flusso di accesso come delegato - introduzione campi “federation” e "protocol" negli endpoint relativi all’onboarding dei Service Provider.	IPZS

Introduzione

Questo allegato tecnico definisce un profilo implementativo dei protocolli di scambio tra Service Provider (SP), Identity Provider (IdP) e la Piattaforma Gestione Deleghe (PGD) per l'ottenimento da parte di un SP di una delega di un Utente.

Linguaggio Normativo e Convenzioni

Le parole chiave "DEVE" e "DEVONO", "NON DEVE" e "NON DEVONO", "RICHIEDE" e "RICHIESTO", "NON DEVE", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "PUÒ" e "OPZIONALE" nel presente documento devono essere interpretate come descritte nel [BCP14] [RFC2119] [RFC8174] quando e solo quando appaiono in maiuscolo.

Flusso High-Level

Nell'ambito dell'utilizzo della PGD sono coinvolti i seguenti attori principali:

- **Service Provider**: sistema che fornisce un servizio online della Pubblica Amministrazione come soggetto fruitore di una delega di un cittadino. È anche sinonimo di Relying Party;
- **Identity Provider**: sistema responsabile dell'identificazione del cittadino che si autentica al fine di accedere ad un servizio online del SP per conto di un soggetto terzo (delegante). Agisce come intermediario nella comunicazione tra SP e PGD;
- **Piattaforma Gestione Deleghe**: sistema che gestisce e fornisce le deleghe dei cittadini e interagisce con l'IdP per consentire al cittadino delegato di accedere per conto di un delegante ad un servizio online di un SP.



Gestione Abilitazione dei Service Provider

Per consentire la creazione e l'utilizzo di una delega per l'accesso ai servizi online di un SP, quest'ultimo DEVE effettuare una procedura tecnica di adesione a PGD secondo quanto definito nelle successive sezioni.

L'onboarding tecnico e la gestione operativa del SP su PGD richiedono l'autenticazione del SP tramite il meccanismo private_key_jwt (RFC7523) e la verifica dell'autenticità tramite confronto con i metadata ufficiali pubblicati dalle fonti autoritative SPID/CIE (AgID e Ministero dell'Interno).

Panoramica del ciclo di vita e delle funzionalità di gestione degli SP

La PGD fornisce un insieme di funzionalità per gestire, la richiesta di abilitazione e il ciclo di vita dei SP abilitati. Il ciclo di vita degli SP si articola nelle seguenti fasi:

1. Onboarding Tecnico: Processo iniziale di abilitazione di un SP al sistema delle deleghe, definito nella sezione "Processo tecnico di abilitazione".
Al completamento dell'onboarding, la PGD rilascia al SP un **Trust Mark JWT**, un'attestazione firmata come prova dell'avvenuta abilitazione del SP a PGD, da conservare nei log come evidenza opponibile a terzi.

2. Operatività
Una volta completato l'onboarding, il SP è inserito nel Registro JWT degli SP abilitati, che viene reso disponibile pubblicamente dalla PGD. Durante le operazioni di autenticazione del cittadino ad un servizio online del SP, gli IdP verificano la presenza del SP nel registro e, se abilitato, mostrano al cittadino l'opzione di accesso con delega.

3. Gestione Continuativa
Durante la fase operativa, il SP può avere la necessità di effettuare operazioni amministrative sulla propria abilitazione. La PGD fornisce API REST dedicate per le seguenti operazioni di gestione:

- **Verifica Stato Abilitazione** (**POST** /pgd/sp/status): Consente al SP di interrogare lo stato corrente della propria abilitazione, la data di onboarding, e l'indirizzo **e-mail** di contatto registrato**;**
- **Modifica Contatti** (PUT /pgd/sp/contact): Consente al SP di aggiornare l'indirizzo **e-mail** di contatto (PEC o **e-mail** istituzionale) utilizzato dalla PGD per le comunicazioni ufficiali**;**
- **Altre operazioni future**: La PGD si riserva di aggiungere ulteriori endpoint di gestione.

Tutti gli endpoint di gestione richiedono autenticazione del SP tramite il meccanismo private_key_jwt come definito nella sezione "Meccanismo di Autenticazione del SP".

4. Offboarding
Quando un SP desidera cessare l'utilizzo delle deleghe o viene revocato dalla PGD, viene avviato il processo di offboarding:

- **Offboarding Volontario**: Il SP richiede la rimozione dal registro PGD tramite endpoint dedicato (**POST** /pgd/sp/offboarding). La rimozione ha effetto **immediato e causa la rigenerazione del registro della PGD;**
- **Offboarding per Revoca**: La PGD revoca unilateralmente l'abilitazione di un SP (es. per violazioni, cessazione dei requisiti di PA, ecc.), rimuovendo l'identificativo del SP dal Registro JWT. In tal caso la PGD notifica il SP usando il canale di contatto registrato.

La revoca ha effetto immediato al successivo refresh del registro da parte degli IdP.
Dopo l'offboarding, il SP non può più utilizzare le API di gestione del ciclo di vita. Gli IdP non mostrano più l'opzione di accesso con delega poiché il SP non è più presente nel Registro JWT.
Il SP può richiedere un nuovo onboarding in qualsiasi momento, ripetendo l'intero processo tecnico di abilitazione.

La sezione seguente descrive in dettaglio il processo tecnico di onboarding, la struttura del Trust Mark JWT e del Registro JWT.
Le specifiche degli endpoint di onboarding/offboarding e di gestione del ciclo di vita dei SP, con il relativo meccanismo di client authentication (private_key_jwt), sono definite nella sezione "Endpoint SP-PGD".

Processo tecnico di abilitazione

Il SP che vuol aderire alla PGD DEVE effettuare una richiesta di abilitazione all'endpoint /pgd/**sp/**onboarding secondo quanto definito nella sezione "Endpoint di Onboarding".

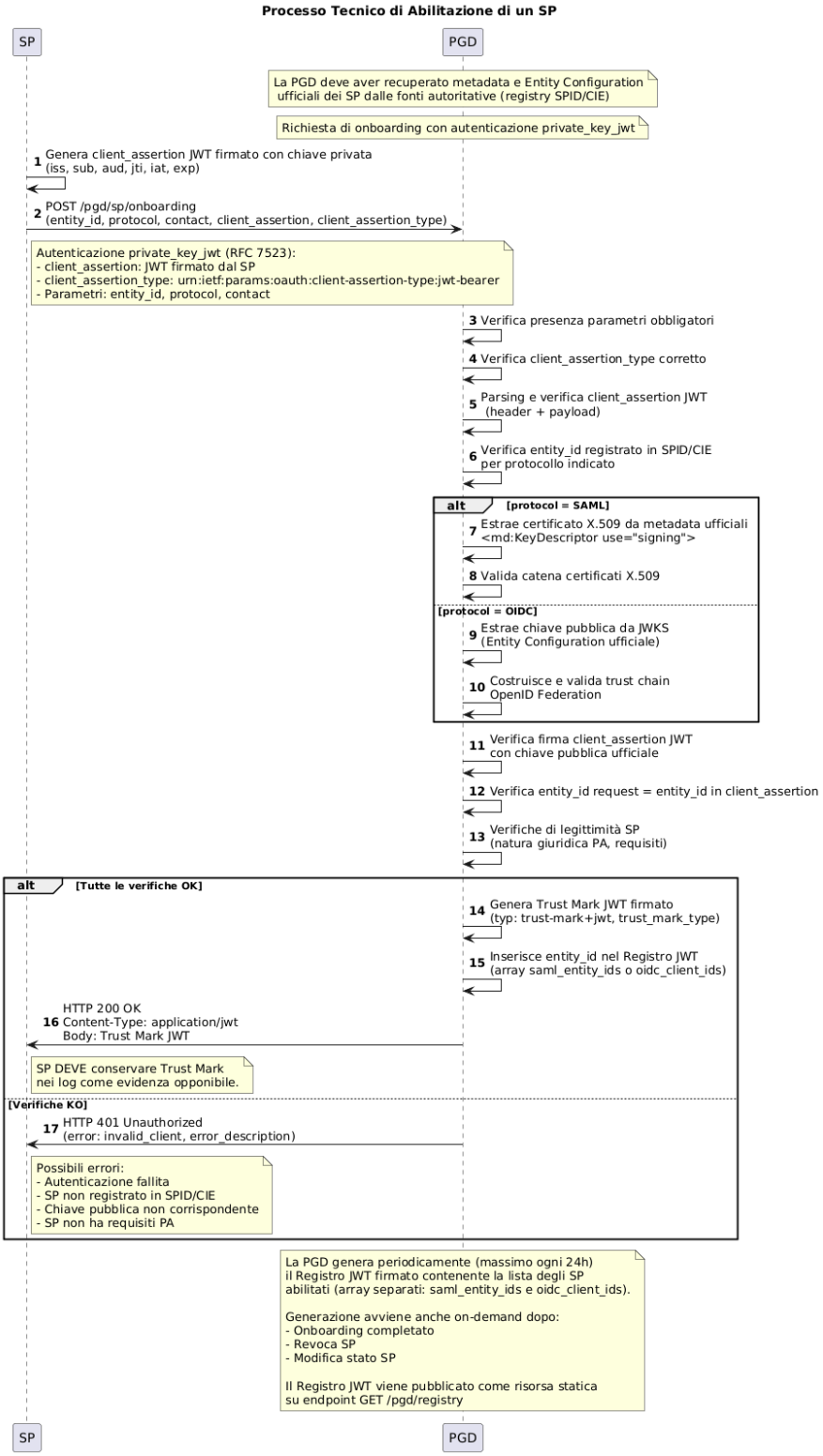


Figura 1 Processo tecnico di abilitazione di un SP.

Come requisito preliminare la PGD DEVE acquisire il materiale crittografico pubblico dei soggetti registrati in SPID e CIE, anche a fronte di eventuali aggiornamenti: per il protocollo SAML i metadata pubblicati nei registri ufficiali SPID/CIE, per il protocollo OIDC le Entity Configuration pubblicate nell'ambito di OpenID Federation, comprensive del JWKS.

Il SP DEVE autenticarsi usando il meccanismo di autenticazione definito nella sezione "Meccanismo di Autenticazione del SP" ed effettuare la richiesta di onboarding tramite l'endpoint POST /pgd/sp/onboarding. La PGD DEVE effettuare le verifiche di sicurezza complete (vedi sezione "Processo di Verifica della PGD") e, se tutte le verifiche hanno esito positivo, rilascia il Trust Mark (vedi sezione "Trust Mark").

Il Trust Mark rilasciato dalla PGD viene utilizzato dal SP esclusivamente come evidenza opponibile a terzi dell'avvenuto onboarding.

Gli aggiornamenti che impattano i meccanismi di abilitazione dei Service Provider DEVONO essere comunicati con un preavviso minimo di 60 giorni agli IdP e ai SP già abilitati, al fine di consentire l'adeguamento dei sistemi.

Il Registro JWT dei SP Abilitati

Al termine del processo tecnico di abilitazione, la PGD DEVE inserire il SP all'interno di un registro centralizzato degli SP abilitati e DEVE rendere disponibile pubblicamente tale registro sotto forma di JWT firmato con validità massima di 24 ore.

Formato del Registro JWT

JWT Header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**pgd-registry+jwt**";
- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma (vedi Sezione "Algoritmi Supportati");
- **kid**: [OBBLIGATORIO]. Stringa. Identificativo della chiave pubblica della PGD utilizzata per la firma in UUID v4.

JWT Payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo della PGD (es. https://**pgd.example.it**);
- **iat**: [OBBLIGATORIO]. Intero. Timestamp Unix di emissione del registro;
- **exp**: [OBBLIGATORIO]. Intero. Timestamp Unix di scadenza del registro. La validità DEVE essere massimo 24 ore (exp - iat ≤ 86400);
- service_providers: [OBBLIGATORIO]. Array di oggetti. Lista degli SP abilitati al servizio deleghe. Ciascun oggetto DEVE contenere entity_id (Stringa), federation (Stringa, valori ammessi spid, cie) e protocol (Stringa, valori ammessi saml, oidc). Puo essere un array vuoto se non ci sono SP abilitati.

Esempio non normativo di Registro JWT:

```
{
  "typ": "pgd-registry+jwt",
  "alg": "ES256",
  "kid": "3f231b99-f6d6-4518-07b9-08d0913fd28d"
}
.
{
  "iss": "https://pgd.example.it",
  "iat": 1734960000,
  "exp": 1735046400,
  "service_providers": [
     { "entity_id": "https://sp1.example.it", "federation": "spid",
"protocol": "saml" },
     { "entity_id": "https://comune.example.it", "federation": "cie",
"protocol": "saml" },
     { "entity_id": "https://sp2.example.it", "federation": "spid",
"protocol": "oidc" }
  ]
}
}
```

Generazione e Aggiornamento del Registro

La PGD DEVE implementare un processo automatico di generazione del Registro JWT che viene eseguito:

- **Periodicamente**: Almeno ogni 24 ore (schedulazione automatica)**;**
- **On-demand**: A seguito di eventi che modificano il registro degli SP (onboarding, revoca SP)**.**

La generazione del Registro JWT DEVE essere attivata nei seguenti casi:

1. **Schedulazione temporale**: Job schedulato che viene eseguito almeno ogni 24 ore**;**
2. **Evento onboarding SP**: Immediatamente dopo il completamento di un onboarding**;**
3. **Evento revoca SP**: Immediatamente dopo la revoca di un SP**.**

La PGD, durante il processo di generazione, DEVE:

1. **Estrarre SP attivi**: Recuperare dal database tutti gli SP con stato active (onboardatinon revocati)
2. **Costruire l'array service_providers**: per ciascun SP attivo inserire un oggetto con entity_id, federation e protocol.
3. **Generare timestamp**:
    - Claim iat: Timestamp Unix corrente (momento di generazione)**;**
    - Claim exp: iat + 86400 (validità 24 ore)**.**
4. **Costruire payload JWT**: Creare il payload del Registro JWT con i claim specificati nella sezione "Formato del Registro JWT"**;**

5. **Firmare JWT**: Firmare il JWT con la chiave privata della PGD utilizzando l'algoritmo specificato nella sezione "Algoritmi Supportati"**;**
6. **Includere kid**: Aggiungere nell'header JWT il claim kid contenente l'identificativo (UUID v4) della chiave pubblica utilizzata per la firma**.**

Dopo la generazione del Registro JWT, la PGD DEVE pubblicarlo come risorsa statica per consentire la distribuzione efficiente agli IdP minimizzando il carico computazionale per richiesta, e renderlo disponibile tramite l'endpoint /pgd/registry (vedi sezione "Endpoint del Registro").

Nel caso di revoca di un SP, la PGD DEVE:

1. Eliminare dal Registro l'oggetto dell'array service_providers corrispondente alla tripla entity_id + federation + protocol del SP revocato, lasciando inalterate eventuali altre registrazioni del medesimo entity_id su federazione o protocollo diversi;
2. Rigenerare il Registro JWT**;**
3. Pubblicare il nuovo Registro JWT come risorsa statica.

La revoca ha effetto immediato e causa il refresh del Registro della PGD.

Verifica dell'abilitazione del SP da parte dell'IdP

La verifica dell'abilitazione del SP da parte degli IdP DEVE avvenire tramite il controllo della presenza, nell'array service_providers del Registro JWT, di un oggetto corrispondente alla tripla entity_id, federation e protocol del SP che la PGD DEVE rendere disponibile tramite l'endpoint /pgd/registry.
All'accesso di uno specifico SP, l'IdP DEVE effettuare le verifiche riportate nella sezione "Endpoint del Registro" utilizzando il Registro JWT.
In caso di esito positivo di tutte le verifiche, dopo l'autenticazione dell'utente, l'IdP DEVE mostrare al cittadino l'opzione di accesso con delega.
In caso di fallimento di una qualsiasi verifica, l'IdP NON DEVE mostrare l'opzione di accesso con delega e DEVE procedere con il normale flusso di autenticazione senza delega.

Le specifiche tecniche complete dell'endpoint del registro sono definite nella sezione "Endpoint del Registro".

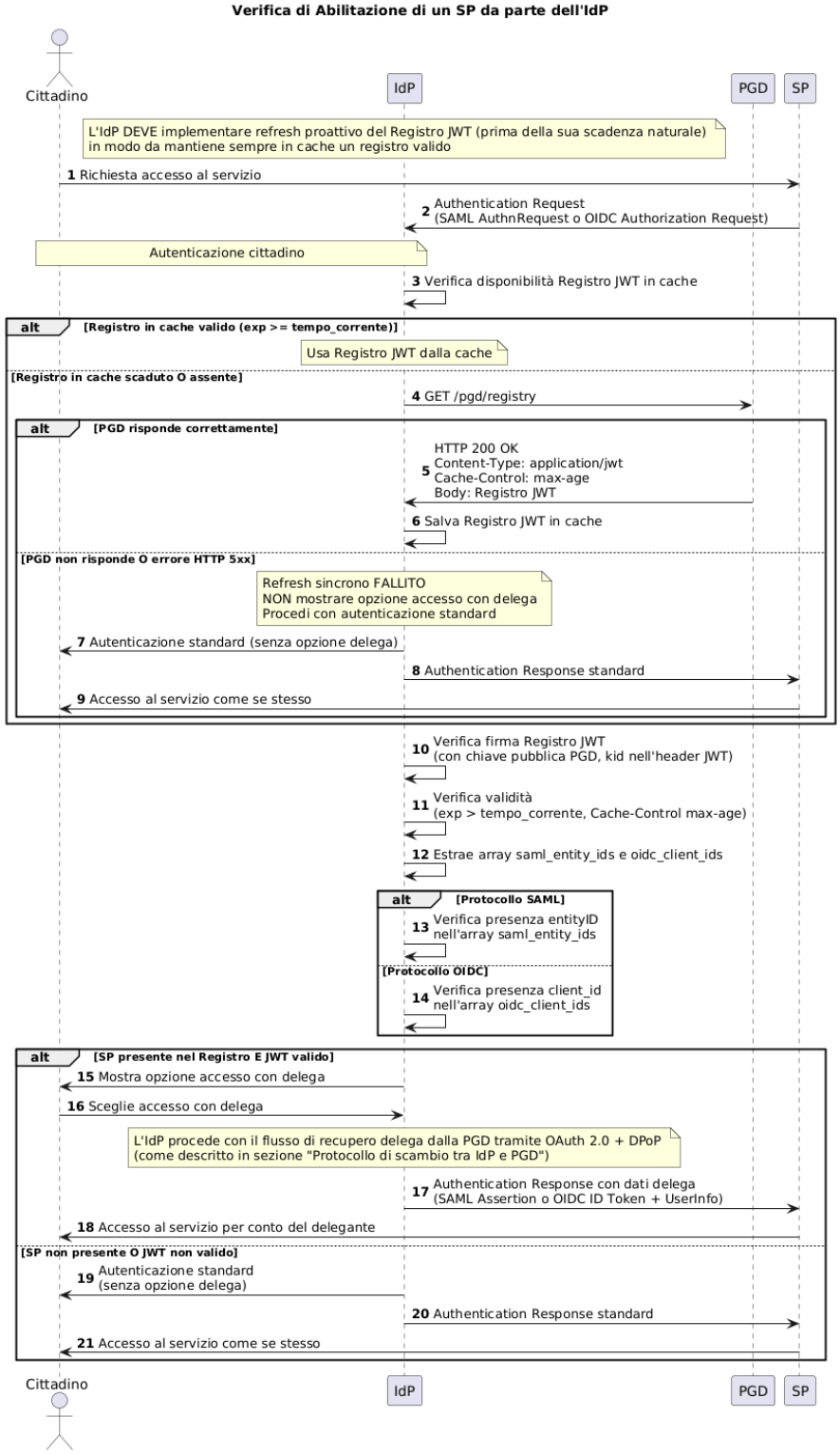


Figura 2 Verifica di abilitazione di un SP da parte di un IdP.

Aggiornamento e Refresh del Registro

La PGD DEVE generare un nuovo Registro JWT ogni 24 ore al massimo, aggiornando automaticamente i timestamp *iat* ed *exp* e includendo l'elenco aggiornato degli SP abilitati (comprensivo di eventuali nuovi onboarding o revoche). Nel caso di revoca di un SP, la PGD DEVE eliminare l'identificativo del SP dal Registro.
Gli IdP DEVONO scaricare il nuovo Registro JWT almeno una volta ogni 24 ore per garantire l'aggiornamento delle abilitazioni. Gli IdP DEVONO implementare un meccanismo di caching locale del Registro JWT con refresh automatico prima della scadenza.

Endpoint SP-PGD

La PGD DEVE esporre endpoint HTTP dedicati per consentire agli SP di effettuare l'onboarding e gestire il proprio ciclo di vita. Tutti gli endpoint DEVONO soddisfare i seguenti requisiti di base:

- Utilizzo del protocollo HTTPS (TLS 1.2 o superiore)**;**
- Autenticazione del SP tramite il meccanismo **private_key_jwt** secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP".

Endpoint	**Metodo**	**Descrizione**
/pgd/sp/onboarding	POST	Onboarding SP e inserimento nel registro dei SP abilitati
/pgd/sp/status	POST	Verifica stato abilitazione SP
/pgd/sp/contact	PUT	Modifica contatti SP
/pgd/sp/offboarding	POST	Offboarding SP dal registro dei SP abilitati

Gli endpoint di onboarding e gestione del ciclo di vita dei SP (/pgd/sp/*) sono definiti nella sezione "Gestione Abilitazione dei Service Provider".

Meccanismo di Autenticazione del SP

Il meccanismo di autenticazione del SP DEVE essere conforme a quanto definito in OAuth 2.0 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC7523] e garantisce:

- **Proof-of-possession**: Il SP dimostra il possesso della chiave privata firmando un JWT (client_assertion) con la propria chiave privata**;**
- **Non-repudiation**: Il JWT firmato costituisce evidenza crittografica dell'autenticazione non ripudiabile**;**
- **Anti-impersonation**: La PGD verifica la firma del JWT utilizzando esclusivamente la chiave pubblica recuperata dai metadata ufficiali SPID/CIE pubblicati dalle fonti autoritative (AgID, Ministero dell'Interno), impedendo attacchi di impersonazione**;**
- **Freshness**: Il JWT ha validità temporale limitata (claim exp, massimo 5 minuti) e contiene un identificativo univoco (claim jti) per prevenire attacchi replay**.**

Struttura del client_assertion JWT

Il SP DEVE generare un JWT (client_assertion) con la seguente struttura:

Header:

- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma. È RACCOMANDATO ES256 (ECDSA con curva P-256 e SHA-256)**;**
- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "pgd-registration-request+jwt";
- **kid**: [OBBLIGATORIO se non presente x5c]. Stringa. Key ID della chiave utilizzata per firmare il JWT. DEVE corrispondere al kid di una chiave pubblica presente nei metadata SPID/CIE del SP**;**
- **x5c**: [OBBLIGATORIO se non presente kid]: Array di stringhe. Catena di certificati X.509 in formato Base64-encoded DER. Il primo certificato DEVE contenere la chiave pubblica utilizzata per firmare il JWT. I certificati successivi (se presenti) DEVONO formare la catena di certificazione.

Payload:

- **iss**: [OBBLIGATORIO]. Stringa. Issuer del JWT. DEVE essere l'entity_id del SP (entityID per SAML, client_id per OIDC)**;**
- **sub**: [OBBLIGATORIO]. Stringa. Subject del JWT. DEVE essere l'entity_id del SP (stesso valore di iss)**;**
- **aud**: [OBBLIGATORIO]. Stringa. Audience del JWT. DEVE essere l'identificativo della PGD (es. https://pgd.**example.**it)**;**
- **jti**: [OBBLIGATORIO]. Stringa. JWT ID. Identificativo univoco del JWT. È RACCOMANDATO utilizzare UUID v4**;**
- **iat**: **[OBBLIGATORIO].** Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Numero (intero). Expiration Time. Timestamp Unix (secondi) di scadenza del JWT. DEVE essere iat + massimo 300 secondi (5 minuti)**.**

Esempio non normativo di client_assertion JWT:

```
{
"alg": "ES256",
"typ": "pgd-registration-request+jwt",
"kid": "NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs"
}.
{
"iss": "https://sp.example.it",
"sub": "https://sp.example.it",
"aud": "https://pgd.example.it/",
"federation": "cie",
"protocol": "saml",
"jti": "a1b2c3d4-e5f6-4789-a012-3456789abcde",
"iat": 1734960000,
"exp": 1734960300
}
```

Invio della client_assertion

Il SP DEVE includere nella richiesta HTTP **(body in formato application/json)** i seguenti parametri:

- **client_assertion**: [OBBLIGATORIO]. Stringa. Il JWT firmato (formato compatto JWT: header.payload.signature)**;**
- **client_assertion_type**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "urn:ietf:params:oauth:client-assertion-type:jwt-bearer".

Esempio non normativo di richiesta HTTP:

```
POST /pgd/sp/status HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol": "saml",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type": "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
}
```

Processo di Verifica della PGD

La PGD, a seguito della ricezione di una richiesta autenticata con private_key_jwt, DEVE effettuare le seguenti verifiche:

1. **Verifica formato client_assertion_type**: Verificare che il parametro client_assertion_type sia valorizzato con "**urn:ietf:params:oauth:client-assertion-type:jwt-bearer**"**;**

2. **Parsing client_assertion JWT**: Decodificare header e payload del JWT (senza ancora verificare la firma)**;**
3. **Verifica claim JWT obbligatori e validità temporale**: Verificare che:
    - iss e sub siano presenti e abbiano lo stesso valore;
    - aud sia presente e corrisponda all'identificativo della PGD (es. https://pgd.example.it);
    - iat ed exp siano presenti. Il valore dello iat NON DEVE essere successivo all'istante in cui viene verificato il JWT;
    - exp - iat <= 300 secondi (massimo 5 minuti di validità);
    - il JWT non sia scaduto (exp > tempo corrente);
    - jti sia presente e non sia già stato utilizzato in una richiesta precedente. La PGD DEVE implementare una cache dei jti già utilizzati, con TTL pari alla massima validità del JWT, e DEVE rifiutare una richiesta il cui jti risulti già presente.
4. **Estrazione chiave pubblica del SP**: Estrarre dai metadata ufficiali la chiave pubblica corrispondente a quella specificata nell'header del client_assertion JWT:
    - **SAML**: Estrazione del certificato X.509 dalla sezione <md:KeyDescriptor use="signing">**;**
    - **OIDC**: Estrazione della chiave pubblica dal JWKS pubblicato nell'Entity Configuration**.**
5. **Verificare che la chiave pubblica estratta sia autentica (tramite la validazione della catena dei certificati x**.509 nel caso SAML, oppure tramite la costruzione e validazione della trust chain OpenID Federation nel caso OIDC)**;**
6. **Verifica firma JWT (anti-impersonation)**: Verificare la firma del client_assertion JWT utilizzando **esclusivamente** la chiave pubblica estratta dai metadata ufficiali della fonte autoritativa.

Se tutte le verifiche hanno esito positivo, la PGD DEVE processare la richiesta.

Gestione errori
In caso di autenticazione non valida, la PGD DEVE rispondere con HTTP status code 401 Unauthorized e il seguente payload JSON:

```
{
"error": "invalid_client",
"error_description": "Invalid client authentication"
}
```

Gestione Chiavi per private_key_jwt

Il SP PUÒ utilizzare una chiave già presente nei propri metadata/Entity Configuration SPID/CIE per firmare il client_assertion JWT. Tuttavia, è RACCOMANDATO generare una nuova coppia di chiavi dedicata esclusivamente all'autenticazione verso PGD, garantendo separation of concerns e facilitando la rotazione indipendente.

Per SAML:
Se il SP genera nuove chiavi dedicate, DEVE:
1. Generare una nuova coppia di chiavi (RACCOMANDATO: ECDSA P-256)**;**
2. Aggiungere la nuova chiave pubblica ai metadata SAML in <md:KeyDescriptor use="signing">**;**

3. Risottomettere i metadata aggiornati ad AgID (per SPID) o Ministero dell'Interno (per CIE) seguendo le procedure previste dalle Regole Tecniche**;**
4. Attendere la validazione e pubblicazione dei metadata aggiornati nei registri ufficiali**;**
5. Solo dopo la pubblicazione dei metadata aggiornati, il SP PUÒ iniziare a utilizzare la nuova chiave per firmare i client_assertion JWT verso PGD**.**

Per OIDC (OpenID Federation):
Se il SP genera nuove chiavi dedicate, DEVE:
1. Generare una nuova coppia di chiavi (RACCOMANDATO: ECDSA P-256)**;**
2. Assegnare un kid descrittivo alla chiave**;**
3. Aggiungere la nuova chiave pubblica al JWKS pubblicato nell'Entity Configuration**;**
4. Aggiornare e ripubblicare l'Entity Configuration**.**

In entrambi i casi, è RACCOMANDATO che il SP utilizzi un kid (Key ID) descrittivo per identificare la chiave dedicata a PGD.

Rotazione Chiavi

Il SP PUÒ ruotare le chiavi utilizzate per private_key_jwt in qualsiasi momento seguendo le procedure previste per l'aggiornamento dei metadata SPID/CIE.

Il SP DOVREBBE seguire la seguente procedura di rotazione:
1. Pubblicare la nuova chiave pubblica nei metadata SPID/CIE (mantenendo anche la vecchia)
2. Attendere la propagazione (per SAML: pubblicazione registry, per OIDC: immediato)
3. Iniziare a utilizzare la nuova chiave privata per firmare i client_assertion JWT
4. Dopo un periodo di overlap, rimuovere la vecchia chiave dai metadata

Questo approccio garantisce che la PGD possa validare sia i JWT firmati con la vecchia chiave (ancora in cache) che quelli firmati con la nuova chiave.

Endpoint di Onboarding

Richiesta HTTP

La richiesta HTTP di onboarding DEVE essere inviata usando il metodo HTTP POST.

HTTP Request Headers:

- **Content-Type:** [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “application/json”.

HTTP Request Body:

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC);
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.

- **protocol**: [OBBLIGATORIO]: Stringa. Protocollo utilizzato dal SP nell'ambito delle federazioni CIE/SPID. Valori ammessi: saml, oidc;
- **email**: [OBBLIGATORIO]: Stringa. Indirizzo e-mail di contatto del SP in formato PEC o e-mail istituzionale della Pubblica Amministrazione;
- **client_assertion**: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT";
- **client_assertion_type**: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo:

```
POST /pgd/sp/onboarding HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol": "saml",
  "email": "sp@pec.example.it",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
 "client_assertion_type":    "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
}
```

Verifiche della PGD

La PGD, a seguito della ricezione della richiesta, DEVE effettuare le seguenti verifiche:

- Verifica che siano presenti tutti i parametri obbligatori della richiesta HTTP.
- Verifica che l'entity_id inviato nella richiesta corrisponda a un SP registrato, per il protocollo indicato, nella federazione specificata nel parametro federation (spid o cie), tramite i metadata ottenuti dal registro ufficiale della federazione corrispondente. La tripla entity_id + federation + protocol identifica univocamente l'istanza di abilitazione del SP.
- Verificare che l'entity_id inviato nella richiesta HTTP corrisponda all'identificativo presente nella client_assertion.
- Verifica la corretta autenticazione del SP secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP", in particolare nella sottosezione "Processo di Verifica della PGD".

Se tutte le verifiche hanno esito positivo, la PGD DEVE:

1. Generare un Trust Mark JWT firmato attestante l'abilitazione del SP
2. Inserire il SP nel Registro JWT degli SP abilitati (array service_providers, come oggetto con entity_id, federation e protocol)
3. Registrare un evento di audit con, a titolo esemplificativo, entity_id, email, timestamp, IP source.
4. Fornire una risposta HTTP con status code 200 contenente il Trust Mark.

Trust Mark

Il Trust Mark JWT DEVE contenere i seguenti claim:

Header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “trust-mark+jwt”;
- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma (vedi Sezione "Algoritmi Supportati");
- **kid**: [OBBLIGATORIO]. Stringa. Identificativo della chiave pubblica della PGD utilizzata per la firma in UUID v4.

Payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo della PGD (es. https://pgd.example.it);
- **sub**: [OBBLIGATORIO]. Stringa. Identificativo del SP (entityID SAML o client_id OIDC);
- **federation**: [OBBLIGATORIO]. Stringa. Federazione presso cui il SP e registrato. Valori ammessi: spid, cie;
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo del SP. Valori ammessi: saml, oidc;
- **iat**: [OBBLIGATORIO]. Intero. Timestamp Unix di emissione del Trust Mark;
- **exp**: [OBBLIGATORIO]. Intero. Timestamp Unix di scadenza del Trust Mark;
- **trust_mark_type**: [OBBLIGATORIO]. Stringa. Identificativo univoco del tipo di Trust Mark (es. https://pgd.example.it/trustmark/delegation-enabled).

Risposta HTTP

La risposta HTTP DEVE avere il parametro Content-Type valorizzato con “**application/jwt**” e DEVE restituire nel body il Trust Mark JWT in formato compatto (header.payload.signature) come riportato nell’esempio non normativo seguente (Successo - 200 OK).

```
HTTP/1.1 200 OK
Content-Type: application/jwt
Cache-Control: no-store

eyJhbGciOiJFUzI1NiIsInR5cCI6InRydXN0LW1hcmsrand0Iiwia2lkIjoicGdkLXRtLWtleS0yM
DI2In0.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJzdWIiOiJodHRwczovL3NwLmV4YW1wbG
Uub3JnIiwidHJ1c3RfbWFya190eXBlIjoiaHR0cHM6Ly9wZ2QuZ292Lml0L3RydXN0bWFyay9kZWx
lZ2F0aW9uLWVuYWJsZWQiLCJpYXQiOjE3MzcxMTA0MDV9.MEUCIQCx2y3z4a5b6c7d8e9f0g1h2i3
j4k5l6m7n8o9p0q1r2s3tATBu4v5w6x7y8z9a0b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q
```

Trust Mark JWT decodificato:

```
{
  "alg": "ES256",
  "typ": "trust-mark+jwt",
  "kid": "pgd-tm-key-2026"
}.
{
  "iss": "https://pgd.example.it",
  "sub": "https://sp.example.it",
  "federation": "cie",
  "protocol": "saml",
  "trust_mark_type": "https://pgd.example.it/trustmark/delegation-enabled",
  "iat": 1737110405
```

```
  "exp": 1768646405
}
```

Gestione Errori

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Gestione Ciclo di Vita

Verifica Stato Abilitazione

La richiesta HTTP di verifica dello stato di adesione del SP DEVE essere inviata all'endpoint /pgd/sp/status usando il metodo GET. Questo endpoint consente al SP di verificare lo stato corrente della propria abilitazione.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "application/json".

HTTP Request Body:

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC);
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **client_assertion**: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT";
- **client_assertion_type**: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
POST /pgd/sp/status HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol": "saml",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
 "client_assertion_type":    "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
}
```

A seguito delle opportune verifiche (client authentication e verifiche di presenza dell'entity_id nel registro degli SP abilitati), PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC). DEVE corrispondere all'entity_id fornito nella richiesta.
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **status**: [OBBLIGATORIO]. Stringa. Stato corrente dell'abilitazione del SP. Valori ammessi: active (SP abilitato e presente nel Registro JWT), suspended (SP temporaneamente sospeso), revoked (SP revocato).
- **onboarding_date**: [OBBLIGATORIO]. Stringa. Data e ora di completamento dell'onboarding del SP. Formato: ISO 8601 UTC (es. 2025-01-14T10:30:00Z).
- **email**: [OBBLIGATORIO]. Stringa. Indirizzo e-mail di contatto del SP registrato in PGD (PEC o e-mail istituzionale).

Di seguito un esempio non normativo della risposta HTTP.

HTTP Response (200 OK):

```
{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol":"saml",
  "status": "active",
  "onboarding_date":"2025-01-14T10:30:00Z",
  "email": "admin@sp.example.it"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Modifica Contatti

La richiesta HTTP di modifica dell'indirizzo e-mail di contatto del SP DEVE essere inviata all'endpoint /pgd/sp/contact usando il metodo PUT. Questo endpoint consente al SP di aggiornare l'indirizzo e-mail di contatto utilizzato dalla PGD per le comunicazioni ufficiali.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "application/json".

HTTP Request Body:

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC);
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **email**: [OBBLIGATORIO]. Stringa. Nuovo indirizzo e-mail di contatto del SP in formato PEC o e-mail istituzionale della Pubblica Amministrazione;
- **client_assertion**: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT";
- **client_assertion_type**: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
PUT /pgd/sp/contact HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol":"saml",
  "email": "nuovo.contatto@pec.example.it",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
 "client_assertion_type":    "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
}
```

A seguito delle opportune verifiche (client authentication, verifiche di presenza dell'entity_id nel registro degli SP abilitati e validità del formato **e-mail**), PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC). DEVE corrispondere all'entity_id fornito nella richiesta;
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **email**: [OBBLIGATORIO]. Stringa. Nuovo indirizzo e-mail di contatto del SP aggiornato con successo;
- **updated_at**: [OBBLIGATORIO]. Stringa. Data e ora dell'aggiornamento. Formato: ISO 8601 UTC (es. 2026-01-17T12:15:30Z).

Di seguito un esempio non normativo della risposta HTTP. HTTP Response (200 OK):

```
{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
```

```
  "protocol":"saml",
  "email": "nuovo.contatto@pec.example.it",
  "updated_at": "2026-01-17T12:15:30Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Offboarding

La richiesta HTTP di offboarding (rimozione dal registro PGD) DEVE essere inviata all'endpoint /pgd/sp/offboarding usando il metodo POST. Questo endpoint consente al SP di richiedere volontariamente la rimozione della propria abilitazione al sistema delle deleghe.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "application/json".

HTTP Request Body:

- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC);
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **client_assertion**: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT";
- **client_assertion_type**: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP

```
POST /pgd/sp/offboarding HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol":"saml",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type": "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
}
```

Processo di verifica della PGD

La PGD, a seguito della ricezione della richiesta, DEVE effettuare le seguenti verifiche:

1. Verificare l'autenticazione del SP tramite private_key_jwt (come definito nella sezione "Meccanismo di Autenticazione del SP")
2. Verificare che l'entity_id nel claim iss/sub del client_assertion corrisponda all'entity_id specificato nel body
3. Verificare che il SP sia attualmente abilitato nel registro PGD per la federazione indicata, individuando l'istanza tramite la triplaentity_id + federation + protocol.

Se tutte le verifiche hanno esito positivo, la PGD DEVE:

1. Marcare il SP come "in offboarding" con timestamp della richiesta
2. Programmare la rimozione dell'identificativo del SP dal Registro JWT (entro massimo 24 ore)
3. Registrare un evento di audit con: entity_id, timestamp, IP source
4. Fornire una risposta HTTP con status code 200 e Content-Type application/json

HTTP Response (200 OK)

A seguito delle opportune verifiche, PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- **status**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**offboarded**";
- **entity_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP rimosso dal registro. DEVE corrispondere all'entity_id fornito nella richiesta;
- **federation**: [OBBLIGATORIO]. Stringa. Federazione di provenienza del SP. Valori ammessi: spid, cie.
- **protocol**: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- **offboarding_date**: [OBBLIGATORIO]. Stringa. Data e ora di ricezione della richiesta di offboarding. Formato: ISO 8601 UTC (es. 2026-01-17T16:00:00Z).

Di seguito un esempio non normativo della risposta HTTP.

```
{
  "status": "offboarded",
  "entity_id": "https://sp.example.it",
  "federation": "cie",
  "protocol":"saml",
  "offboarding_date": "2026-01-17T16:00:00Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Protocolli di comunicazione

Nelle sezioni seguenti viene dettagliato l'intero protocollo di comunicazione tra i vari attori del sistema che prevede, in particolare, le seguenti macro-fasi:

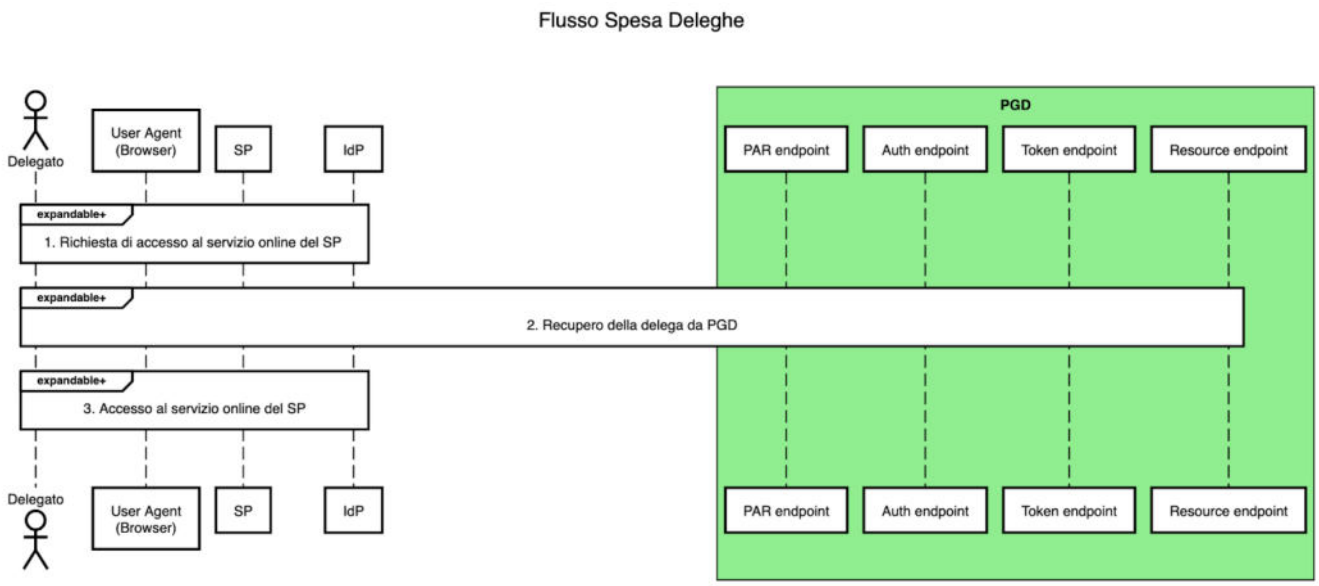
1. Richiesta di accesso al servizio online di un SP;
2. Recupero delle delega da PGD;
3. Accesso al servizio online del SP.

Le fasi 1) e 3) sono dettagliate nella Sezione “Protocollo di scambio tra SP e IdP”.
Il protocollo di scambio relativo alla fase 2) è descritto nella Sezione “Protocollo di scambio tra IdP e PGD”.

In particolare, quest'ultimo protocollo fornisce tutti gli strumenti utili a mitigare i seguenti attacchi:

- **MiTM (Man in the Middle):** Un attaccante si posiziona tra due parti comunicanti intercettando e potenzialmente modificando il traffico. Il protocollo mitiga questo attraverso l'uso di Proof of Possession che lega il token al possessore originale della richiesta di autenticazione, utilizza Client Assertion con JWT firmati per autenticare le richieste tra componenti e richiede un canale TLS esplicito per tutti gli endpoint;
- **Replay Attack**: L'attaccante cattura una comunicazione valida e la ri-trasmette in un secondo momento per replicare un'azione autorizzata. La mitigazione avviene tramite l'inclusione del parametro "jti" (JWT ID) univoco in ogni token e l'uso di parametri temporali "iat", "exp", "nbf" in tutti i JWT;
- **Malicious Administrator:** Un amministratore con privilegi elevati abusa del proprio accesso per compromettere il sistema. Il protocollo richiede l’inserimento di un OTP da parte del delegato durante il processo di utilizzo della delega;
- **Token Theft**: Un attaccante riesce a rubare un token di accesso valido e tenta di utilizzarlo. La mitigazione è effettuata attraverso il binding del token al client specifico tramite DPoP, la verifica della Proof of Possession per ogni richiesta protetta e la limitazione dello scope dei token alle sole operazioni di delega;
- **CSRF (Cross-Site Request Forgery)**: Un attaccante inganna un utente autenticato per fargli eseguire azioni non intenzionali. Il protocollo mitiga questo attraverso l'uso obbligatorio del parametro “state” nelle richieste di autorizzazione, la verifica della corrispondenza dello “state” tra richiesta e risposta, e l'obbligo di generare valori “state” casuali con entropia sufficiente (minimo 32 caratteri).
- **Mix-Up Attack**: Un attaccante inganna l'applicazione facendole scambiare informazioni sensibili con un server di identità malevolo mentre l'utente si autentica correttamente con un provider legittimo. Il protocollo mitiga questo attacco introducendo l’identificativo univoco della PGD nella Authorization Response richiedendo che l’IdP verifichi che tutte le richieste del flusso di autenticazione siano correttamente dirette alla PGD, confrontando gli identificativi univoci ad ogni passo.

Inoltre, il protocollo mitiga potenziali rischi di privacy limitando l'accesso dell'IdP alla sola delega selezionata dall'utente (e non all'intera lista delle deleghe a lui assegnate), e, in ogni caso, solo a seguito di un esplicito consenso dell’utente a comunicare tali dati all'IdP.
Segue il diagramma di alto livello del protocollo.



Nelle interazioni tra Piattaforma Gestione Deleghe (PGD), Identity Provider (IdP) e Service Provider (SP) i dati relativi ai soggetti delegante e delegato, trasmessi all'interno dei flussi di autenticazione (SAML e OIDC), DEVONO essere limitati a quanto richiesto dal SP in fase di autenticazione, secondo le capacità degli specifici protocolli di autenticazione e con gli stessi attributi sia per il delegante che per il delegato.

Protocollo di scambio tra SP e IdP

Per i dettagli implementativi e gli aspetti normativi del protocollo descritto per i flussi “Richiesta di accesso al servizio online dei SP” e “Accesso al servizio online del SP” del precedente diagramma, si rimanda alle specifiche tecniche di autenticazione Regole Tecniche CIE eID SAML, Regole Tecniche SPID SAML e SPID/CIE OpenID Connect Regole tecniche.

Viene comunque di seguito riportato lo schema delle chiamate necessarie ad implementare i due flussi per dare evidenza delle necessarie differenze introdotte allo scopo di integrare la PGD nel sistema di autenticazione.

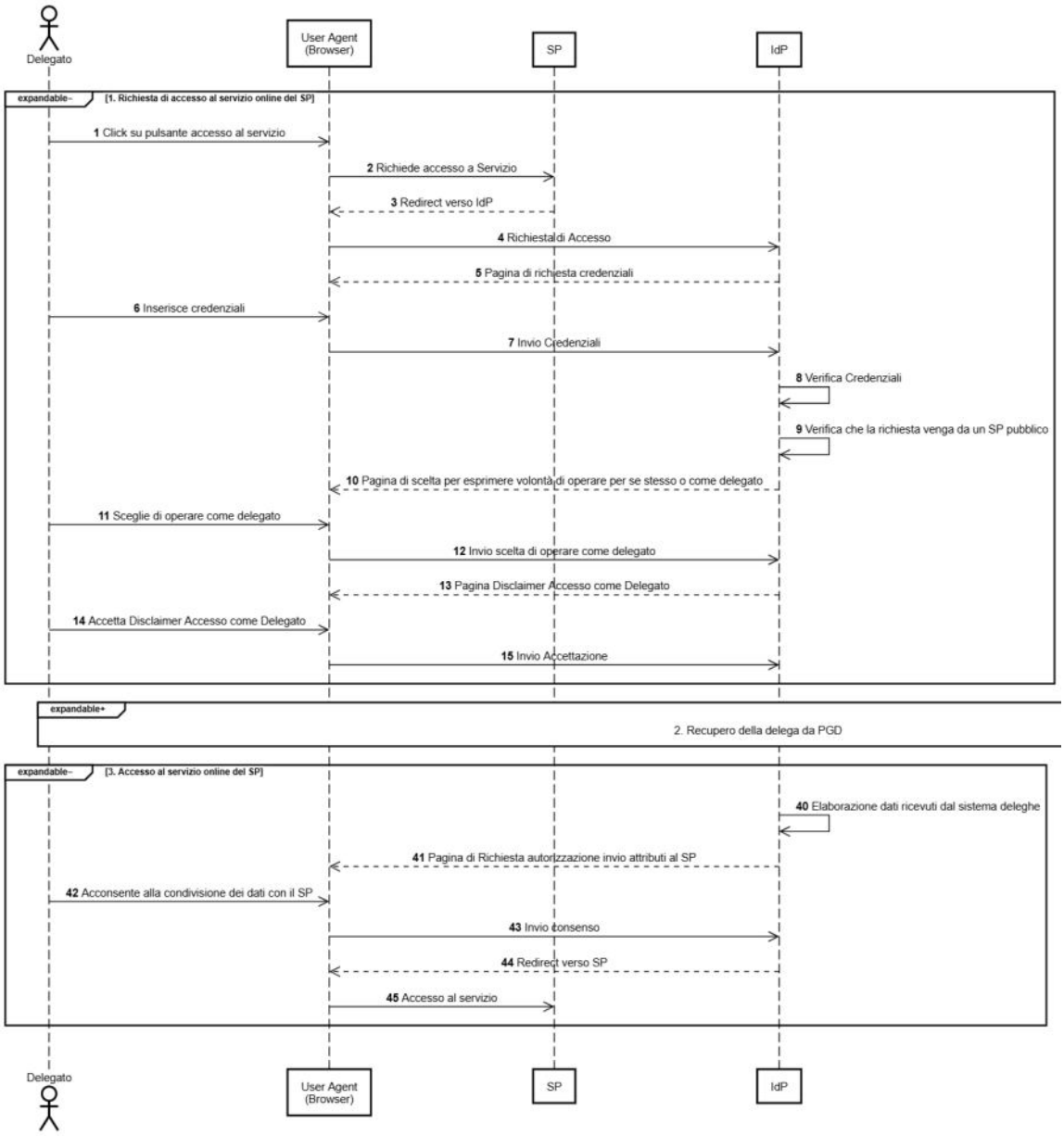


Figura 3 Protocollo di scambio tra SP e IdP.

Alla ricezione di una richiesta di accesso, l'IdP DEVE verificare che il SP che ha generato la richiesta abbia aderito alla PGD e che sia parte della Pubblica Amministrazione.
La verifica di adesione deve essere effettuata secondo quando descritto al paragrafo Gestione Abilitazione dei Service Provider.

Successivamente l'IdP DEVE verificare l'intenzione dell'utente che sta effettuando l'autenticazione come delegato e DEVE informarlo delle implicazioni legali che tale scelta comporta (Disclaimer). In tale fase e

comunque prima dell'avvio delle interazioni con la PGD, l'IdP DEVE rendere direttamente accessibile all'utente la propria informativa sul trattamento dei dati personali. Le informazioni relative alle implicazioni dell'accesso in qualità di delegato (Disclaimer) e l'informativa sul trattamento dei dati personali POSSONO essere rese dall'IdP contestualmente nella schermata in cui l'utente sceglie di operare come delegato, in ogni caso prima che sia effettuato l'accesso come delegato.

Al termine del flusso di autenticazione l'IdP DEVE inoltre raccogliere l'autorizzazione dell'utente ad inviare i dati della delega (nello specifico i dati anagrafici del delegante e del delegato) al SP che ha originato la richiesta di autenticazione.

Infine, l'accesso ai dati di delega deve disabilitare qualsiasi meccanismo di rinnovo della sessione tra IdP e SP, sia in SAML, sia in OIDC. Questo per non consentire il riutilizzo dei dati della delega senza aver richiesto una nuova autenticazione utente e senza aver richiesto le opportune verifiche di validità della delega sulla PGD.
In caso di accesso come delegato, DEVE quindi essere disabilitata la generazione e propagazione dei "refresh_token" per OIDC.
Mentre per quanto riguarda SAML DEVONO essere configurati valori fissi e brevi per il parametro "SessionNotOnOrAfter", il parametro "ForceAuthn" DEVE essere valorizzato a "true" e DEVONO essere disabilitati anche eventuali meccanismi di keep-alive lato IdP.

Questo è necessario per evitare che un'autenticazione possa essere riutilizzata per ottenere nuovi dati di delega senza richiedere una nuova autenticazione utente.

La PGD DEVE limitare il proprio funzionamento ai soli accessi effettuati con un livello di garanzia pari o superiore a «significativo» (substantial) ai sensi del Regolamento eIDAS e dell'Art. 64 ter, comma 1 del CAD.
Pertanto, qualora la richiesta di autenticazione originata dal SP preveda un livello di garanzia inferiore a «significativo», l'IdP NON DEVE mostrare al cittadino l'opzione di accesso con delega e la PGD NON DEVE erogare i dati della delega.

OIDC

Nel protocollo OIDC, a seguito di una richiesta di accesso ad un Relying Party (RP), viene generata una Authorization Request che una volta inviata all'IdP avvia il flusso di autenticazione utente.

Al termine del flusso di autenticazione, il RP ottiene dall'IdP (quest'ultimo anche denominato OpenID Provider) un "access_token" tramite il quale può invocare l'endpoint /userInfo per accedere ai dati dell'utente che si è autenticato.

In aggiunta ai parametri definiti nelle Regole Tecniche OIDC per SPID e CIE id, con l'introduzione della PGD, l'OpenID Provider (OP) DEVE inviare al RP i seguenti parametri:

- **is_delegate**: [OBBLIGATORIO]. Booleano. Valorizzato a true se l'utente ha effettuato l'accesso con delega e a false altrimenti;
- **delegation_info**: [CONDIZIONALE]. Stringa. Se is_delegate è valorizzato a true, DEVE contenere il payload del JWT delegation_info restituito dalla PGD.

In caso di accesso come delegato tutti gli attributi identificativi dell'utente richiesti dal RP DEVONO essere valorizzati con i dati del delegante (e non con i dati dell'utente che ha effettuato l'accesso e inserito le credenziali).
Nel contesto "CIE ID" gli attributi dell'utente sono disponibili sia nell'ID Token, sia nella UserInfo Response. Nei casi in cui ID Token e UserInfo siano equivalenti, quanto appena descritto per la UserInfo, quindi, DEVE valere anche per l'ID Token.

Segue un esempio non normativo della risposta in caso di accesso con delega:


```
{
      "name": "Giuseppe",
      "family_name": "Verdi",
      "birth_date": "1975-05-20",
      "https://attributes.spid.gov.it/fiscal_number": "MROXXXXXXXXXXXXX",
      "is_delegate": true,
      "delegation_info":"eyJ0eXAiOiJwZ2QtZGVsZWdhdGlvbi1kYXRhLXJlc3BvbnNlK2p3
dCIsImFsZyI6IkVTMjU2Iiwia2lkIjoiM2YyMzFiOTktZjZkNi00NTE4LTA3YjktMDhkMDkxM2ZkM
jhkIn0.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJhdWQiOiJodHRwczovL2lkcC5leGFtcG
xlLm9yZyIsInZlcnNpb24iOiIxLjAiLCJkZWxlZ2F0ZSI6eyJuYW1lIjoiTWFyaW8iLCJmYW1pbHl
fbmFtZSI6IlJvc3NpIiwiYmlydGhkYXRlIjoiMTk2NS0xMi0xMCIsImZpc2NhbF9udW1iZXIiOiJS
U1NNUkE2NVQxMEgwMjdYIn0sImRlbGVnYXRvciI6eyJuYW1lIjoiR2l1c2VwcGUiLCJmYW1pbHlfb
mFtZSI6IlZlcmRpIiwiYmlydGhkYXRlIjoiMTk3NS0wNS0yMCIsImZpc2NhbF9udW1iZXIiOiJWUk
RHUFA3NUUyMEYyMDVBIn0sInR5cGUiOiJwYXJlbnRhbF9yZXNwb25zaWJpbGl0eSIsImlhdCI6MTc
zMTg1MzYzNCwibmJmIjoxNzMxODUzNjM0LCJleHAiOjE3MzE4NTcyMzR9.signature"
}
```


SAML

Nel protocollo SAML, a seguito di una richiesta di accesso ad un SP viene generata una AuthnRequest che una volta inviata all'IdP avvia il flusso di autenticazione utente.

Al termine del flusso di autenticazione il SP ottiene una SAML Response dall'IdP contenente una "<saml:Assertion>" con i dati dell'utente autenticato.
.
In aggiunta ai parametri definiti nelle Regole Tecniche SAML per SPID e CIE eID, con l'introduzione della PGD, l'IdP DEVE inviare al SP i seguenti parametri:

- **isDelegate**: [OBBLIGATORIO]. Valorizzato a true se l'utente ha effettuato l'accesso con delega e false altrimenti;
- **delegationInfo**: [CONDIZIONALE]. Oggetto. Se is_delegate è valorizzato a true, DEVE contenere i seguenti parametri estratti dal delegation_info restituito dalla PGD:
    - **jwt**: [OBBLIGATORIO]. Stringa. DEVE contenere il JWT così come ottenuto da PGD durante il flusso di richiesta della delega per consentire ai SP di effettuare la verifica di autenticità delle informazioni di delega;
    - **delegate**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegato**:**
        - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegato;
        - **familyName**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegato;
        - **dateOfBirth**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegato nel formato ISO 8601 (YYYY-MM-DD);

        - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo e-mail del delegato se disponibile;
        - **fiscalNumber**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegato.
    - **delegator**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegante;
        - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegante;
        - **familyName**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegante;
        - **dateOfBirth**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegante nel formato ISO 8601 (YYYY-MM-DD);
        - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo **e-mail** del delegante se disponibile;
        - **fiscalNumber**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegante.
    - **type**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo del tipo di delega conferita al delegato *(vedere tab. 1)*;
    - **iat**: [OBBLIGATORIO]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di emissione del token. Il tipo XML associato è xs:dateTime;
    - **created_at: [OBBLIGATORIO].** Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di creazione della delega. Il tipo XML associato è xs:dateTime;
    - **nbf**: [OPZIONALE]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di inizio validità. Il tipo XML associato è xs:dateTime;
    - **exp**: [OBBLIGATORIO]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di scadenza. Il tipo XML associato è xs:dateTime.

In caso di accesso come delegato, tutti gli attributi identificativi dell'utente richiesti dal SP DEVONO essere valorizzati con i dati del delegante (e non con i dati dell'utente che ha effettuato l'accesso e inserito le credenziali).

Segue un esempio non normativo di Attribute Statement in caso di accesso con delega.

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                          xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

  <!-- Attributi utente autenticato (delegato) -->
  <saml2:Attribute FriendlyName="Nome" Name="name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">Giuseppe</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome" Name="familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
```

```
    <saml2:AttributeValue
xsi:type="xs:string">Verdi</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data di Nascita" Name="dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1975-05-
20</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Codice Fiscale" Name="fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">TINIT-
RSSMRA65T10H027X</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Flag: utente accede come delegato -->
  <saml2:Attribute FriendlyName="Accede come Delegato" Name="isDelegate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xsi:type="xs:boolean">true</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- ======================================== -->
  <!-- DelegationInfo - Attributi destrutturati  -->
  <!-- ======================================== -->

  <saml2:Attribute FriendlyName="Versione Delega"
Name="delegationInfo.version"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1.0</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Informazioni Delegato -->
  <saml2:Attribute FriendlyName="Nome Delegato"
Name="delegationInfo.delegate.name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Mario</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome Delegato"
Name="delegationInfo.delegate.familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Rossi</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data di Nascita Delegato"
Name="delegationInfo.delegate.dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1965-12-
10</saml2:AttributeValue>
  </saml2:Attribute>
```

```
  <saml2:Attribute FriendlyName="Codice Fiscale Delegato"
Name="delegationInfo.delegate.fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">RSSMRA65T10H027X</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Informazioni Delegante -->
  <saml2:Attribute FriendlyName="Nome Delegante"
Name="delegationInfo.delegator.name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">Giuseppe</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome Delegante"
Name="delegationInfo.delegator.familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Verdi</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data di Nascita Delegante"
Name="delegationInfo.delegator.dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1975-05-
20</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Codice Fiscale Delegante"
Name="delegationInfo.delegator.fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">VRDGPP75E20F205A</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Metadata Delega -->
  <saml2:Attribute FriendlyName="Tipo di Delega" Name="delegationInfo.type"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">parental_authority_holder</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data Creazione Delega" Name="delegationInfo.
created_at" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T14:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

<saml2:Attribute FriendlyName="Data Emissione Token"
Name="delegationInfo.iat" NameFormat="...">
  <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T15:33:54Z</saml2:AttributeValue>
</saml2:Attribute>
```

```
  <saml2:Attribute FriendlyName="Data Inizio Validità Delega"
Name="delegationInfo.nbf" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T14:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data Fine Validità Delega"
Name="delegationInfo.exp" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T15:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- ======================================== -->
  <!-- JWT completo firmato da PGD              -->
  <!-- ======================================== -->

  <saml2:Attribute FriendlyName="Delegation Info JWT"
Name="delegationInfo.jwt" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
    <saml2:AttributeValue
xsi:type="xs:string">eyJ0eXAiOiJwZ2QtZGVsZWdhdGlvbi1kYXRhLXJlc3BvbnNlK2p3dCIs
ImFsZyI6IkVTMjU2Iiwia2lkIjoiM2YyMzFiOTktZjZkNi00NTE4LTA3YjktMDhkMDkxM2ZkMjhkI
n0.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJhdWQiOiJodHRwczovL2lkcC5leGFtcGxlLm
9yZyIsInZlcnNpb24iOiIxLjAiLCJkZWxlZ2F0ZSI6eyJuYW1lIjoiTWFyaW8iLCJmYW1pbHlfbmF
tZSI6IlJvc3NpIiwiYmlydGhkYXRlIjoiMTk2NS0xMi0xMCIsImZpc2NhbF9udW1iZXIiOiJSU1NN
UkE2NVQxMEgwMjdYIn0sImRlbGVnYXRvciI6eyJuYW1lIjoiR2l1c2VwcGUiLCJmYW1pbHlfbmFtZ
SI6IlZlcmRpIiwiYmlydGhkYXRlIjoiMTk3NS0wNS0yMCIsImZpc2NhbF9udW1iZXIiOiJWUkRHUF
A3NUUyMEYyMDVBIn0sInR5cGUiOiJwYXJlbnRhbF9yZXNwb25zaWJpbGl0eSIsImlhdCI6MTczMTg
1MzYzNCwibmJmIjoxNzMxODUzNjM0LCJleHAiOjE3MzE4NTcyMzR9.signature</saml2:Attrib
uteValue>
  </saml2:Attribute>

</saml2:AttributeStatement>
```

Onboarding e integrazione dell'IdP con la PGD

Analogamente a quanto previsto per i SP, prima di poter interagire con gli endpoint IdP-PGD l'IdP DEVE completare una procedura tecnica di onboarding sulla PGD. L'onboarding consente alla PGD di censire l'IdP, registrare il materiale crittografico necessario a garantire integrità e confidenzialità delle comunicazioni PGD-IdP e stabilire un canale di contatto per le comunicazioni operative.
La PGD DEVE inoltre esporre gli endpoint necessari alla gestione del ciclo di vita del materiale crittografico dell'IdP e della relativa abilitazione, definiti nelle sezioni seguenti.

La procedura definisce in modo tracciabile lo scambio delle chiavi tra le parti.

Poiché in fase di onboarding l'IdP non è ancora registrato presso la PGD, l'autenticazione della richiesta avviene con le stesse modalità previste per l'onboarding dei SP: la PGD verifica la firma della client_assertion utilizzando la chiave pubblica dell'IdP recuperata esclusivamente dai metadata ufficiali SPID/CIE pubblicati dalle fonti autoritative (AgID, Ministero dell'Interno).

Le medesime modalità di autenticazione DEVONO essere utilizzate per tutti gli endpoint di gestione del ciclo di vita dell'IdP (/pgd/idp/*). La client_assertion inviata a tali endpoint DEVE quindi essere verificata dalla PGD esclusivamente con la chiave pubblica dell'IdP estratta dai metadata ufficiali SPID/CIE, e NON DEVE essere verificata con le chiavi registrate presso la PGD tramite l'onboarding. Queste ultime sono utilizzate unicamente per la client authentication verso gli endpoint di protocollo (PAR e Token), secondo quanto definito nella sezione "Client Authentication". La separazione delle due fonti di fiducia garantisce che la compromissione delle chiavi registrate presso la PGD non consenta a un attaccante di aggiungerne o rimuoverne autonomamente.
Il kid di ciascuna chiave registrata per le comunicazioni IdP-PGD DEVE essere valorizzato con il JWK thumbprint della chiave, calcolato secondo [RFC7638]. Tale vincolo garantisce l'univocità del kid e previene collisioni tra chiavi di soggetti diversi. Il vincolo si applica esclusivamente al materiale crittografico registrato presso la PGD per le comunicazioni IdP-PGD e NON si applica alle chiavi delle federazioni SPID/CIE, per le quali il kid è definito dalle rispettive fonti autoritative.

Endpoint di Onboarding dell'IdP

La richiesta HTTP di onboarding DEVE essere inviata all'endpoint /pgd/idp/onboarding usando il metodo POST.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “application/json”.

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP (entityID per SAML, issuer per OIDC).
- protocol: [OBBLIGATORIO]: Stringa. Protocollo utilizzato dall’IdP nell’ambito delle federazioni CIE/SPID. Valori ammessi: saml, oidc
- authority: [OBBLIGATORIO]. Stringa. Autorità di riferimento per l'accreditamento dell'IdP. Valori ammessi: agid (SPID), min_interno (CIE);
- jwks: [OBBLIGATORIO]. Oggetto JSON. JWK Set contenente le chiavi pubbliche di firma dell'IdP utilizzate nelle comunicazioni PGD-IdP, conforme a [RFC7517]. Le chiavi DEVONO

essere contenute nel membro keys e il kid di ciascuna chiave DEVE essere valorizzato con il JWK thumbprint della chiave, calcolato secondo [RFC7638];

- proofs: [OBBLIGATORIO]. Array di JWT. Insieme delle prove di possesso delle chiavi pubbliche di firma dell'IdP (JWK Set) utilizzate nelle comunicazioni PGD-IdP, definite come descritto nella sezione “DPoP Proof”.
- email: [OBBLIGATORIO]. Stringa. Indirizzo e-mail di contatto dell'IdP in formato PEC o e-mail istituzionale, utilizzato dalla PGD per le comunicazioni ufficiali (es. rotazione delle chiavi);
- redirect_uris: [OBBLIGATORIO]. Array di stringhe. Elenco degli URL di redirezione (redirect_uri) autorizzati per l'IdP nel flusso di autorizzazione verso la PGD. Ciascun valore DEVE essere un URL HTTPS assoluto;
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP con la propria chiave privata per l'autenticazione, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”.

Esempio non normativo della richiesta HTTP:

```
POST /pgd/idp/onboarding HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "protocol": "saml",
  "authority": "agid",
  "jwks": { "keys": [ { "kty": "EC", "crv": "P-256", "kid": "…", "use": "sig",
"x": "…", "y": "…" } ] },
  "proofs": [ "eyJ0eXAiOiJkcG9wK2p3dC…", "eyJ0eXAiOiJkcG9wK2p3dC…" ],
  "email": "idp@pec.example.it",
  "redirect_uris": [ "https://idp.example.it/callback" ],
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type":   "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
```

Verifiche della PGD. La PGD, a seguito della ricezione della richiesta, DEVE:

- verificare che siano presenti tutti i parametri obbligatori;
- verificare che l'entity_id corrisponda a un IdP registrato nella federazione CIE/SPID per il protocollo indicato, tramite i metadata ottenuti dai registri ufficiali;
- verificare la corretta autenticazione dell'IdP secondo il meccanismo private_key_jwt definito nella sezione "Meccanismo di Autenticazione del SP" (sottosezione "Processo di Verifica della PGD"), verificando la firma della client_assertion con la chiave pubblica dell'IdP estratta dai metadata ufficiali SPID/CIE (fonte autoritativa AgID / Ministero dell'Interno);

- validare il contenuto dell'array proofs utilizzando le relative chiavi presenti nel membro keys del JWK Set jwks;
- verificare la coerenza del materiale crittografico fornito e la validità del formato dell'indirizzo e-mail.

Se tutte le verifiche hanno esito positivo, la PGD DEVE registrare l'IdP con il relativo materiale crittografico e contatto, registrare un evento di audit (a titolo esemplificativo: entity_*id, email*, timestamp, IP source) e fornire una risposta HTTP con status code 200 e Content-Type application/json, contenente i seguenti parametri:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP. DEVE corrispondere all'entity_id fornito nella richiesta;
- protocol: [OBBLIGATORIO]. Stringa. Protocollo dell'IdP. Valori ammessi: saml, oidc;
- authority: [OBBLIGATORIO]. Stringa. Autorità di riferimento registrata. Valori ammessi: agid, min_interno;
- status: [OBBLIGATORIO]. Stringa. Stato dell'IdP a valle dell'onboarding. Valore: active.
- onboarding_date: [OBBLIGATORIO]. Stringa. Data e ora di completamento dell'onboarding. Formato: ISO 8601 UTC;
- email: [OBBLIGATORIO]. Stringa. Indirizzo e-mail di contatto registrato in PGD.

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "entity_id": "https://idp.example.it",
 "protocol": "saml",
 "authority": "agid",
 "status": "active",
 "onboarding_date": "2026-01-17T10:30:00Z",
 "email": "idp@pec.example.it"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Verifica Stato dell'IdP

La richiesta HTTP di verifica dello stato di abilitazione DEVE essere inviata all'endpoint /pgd/idp/status usando il metodo POST. Questo endpoint consente all'IdP di verificare lo stato corrente della propria

abilitazione e l'elenco delle chiavi effettivamente registrate presso la PGD, a valle di una sequenza di operazioni di aggiunta e rimozione.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "application/json".

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP (entityID per SAML, issuer per OIDC);
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
POST /pgd/idp/status HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type":   "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
```

A seguito delle opportune verifiche di client authentication e di presenza dell'entity_id tra gli IdP registrati, la PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP. DEVE corrispondere all'entity_id fornito nella richiesta;
- protocol: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dall'IdP. Valori ammessi: saml, oidc;
- authority: [OBBLIGATORIO]. Stringa. Autorità di riferimento registrata. Valori ammessi: agid, min_interno;
- status: [OBBLIGATORIO]. Stringa. Stato corrente dell'abilitazione dell'IdP. Valori ammessi: active (IdP abilitato e operativo), suspended (IdP temporaneamente sospeso), offboarded (IdP non più abilitato);
- onboarding_date: [OBBLIGATORIO]. Stringa. Data e ora di completamento dell'onboarding. Formato: ISO 8601 UTC;

- kids: [OBBLIGATORIO]. Array di stringhe. Elenco dei kid delle chiavi attualmente registrate per l'IdP;
- email: [OBBLIGATORIO]. Stringa. Indirizzo e-mail di contatto registrato in PGD.

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "entity_id": "https://idp.example.it",
 "protocol": "saml",
 "authority": "agid",
 "status": "active",
 "onboarding_date": "2026-01-17T10:30:00Z",
 "kids":        ["NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xsidp-sig-2026-01",
"NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9X"],
 "email": "idp@pec.example.it"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Modifica Contatti dell'IdP

La richiesta HTTP di modifica dell'indirizzo e-mail di contatto dell'IdP DEVE essere inviata all'endpoint /pgd/idp/contact usando il metodo PUT. Questo endpoint consente all'IdP di aggiornare l'indirizzo e-mail di contatto utilizzato dalla PGD per le comunicazioni ufficiali.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “application/json”.

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP (entityID per SAML, issuer per OIDC);
- email: [OBBLIGATORIO]. Stringa. Nuovo indirizzo e-mail di contatto dell'IdP in formato PEC o e-mail istituzionale;
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
PUT /pgd/idp/contact HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "email": "nuovo.contatto@pec.example.it",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type":   "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
}
```

A seguito delle opportune verifiche (client authentication, presenza dell'entity_id tra gli IdP registrati e validità del formato e-mail), la PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json, restituendo entity_id, email aggiornato e updated_at (ISO 8601 UTC).

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "entity_id": "https://idp.example.it",
 "email": "nuovo.contatto@pec.example.it",
 "updated_at": "2026-01-17T12:15:30Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Gestione del Materiale Crittografico dell'IdP

La PGD DEVE consentire all'IdP di aggiungere e rimuovere le chiavi pubbliche registrate durante l'onboarding, senza necessità di ripetere l'intera procedura di abilitazione. A tal fine la PGD DEVE esporre due sole operazioni primitive, di aggiunta e di rimozione, componendo le quali si realizzano sia la rotazione, sia la revoca delle chiavi, come descritto nella sezione "Rotazione e Revoca delle Chiavi".
In ogni momento il materiale crittografico registrato presso la PGD per un IdP è costituito dall'insieme delle chiavi aggiunte e non successivamente rimosse. La PGD DEVE accettare come valide le firme prodotte con una qualsiasi delle chiavi registrate.

Aggiunta di Chiavi

La richiesta HTTP di aggiunta di una o più chiavi DEVE essere inviata all'endpoint /pgd/idp/keys usando il metodo POST.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “application/json”.

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP (entityID per SAML, issuer per OIDC);
- jwks: [OBBLIGATORIO]. Oggetto JSON. JWK Set contenente le chiavi pubbliche di firma che l'IdP intende aggiungere al materiale crittografico già registrato, conforme a [RFC7517]. Le chiavi DEVONO essere contenute nel membro keys e il kid di ciascuna chiave DEVE essere valorizzato con il JWK thumbprint della chiave, calcolato secondo [RFC7638];
- proofs: [OBBLIGATORIO]. Array di JWT. Insieme delle prove di possesso delle chiavi private corrispondenti alle chiavi pubbliche presenti in jwks, definite come descritto nella sezione "DPoP Proof". DEVE essere presente una prova per ciascuna chiave dichiarata in jwks;
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP con la propria chiave privata per l'autenticazione, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”.

Esempio non normativo della richiesta HTTP:

```
POST /pgd/idp/keys HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "jwks": { "keys": [ { "kty": "EC", "crv": "P-256", "kid": "NzbLsXh8uDCcd-
6MNwXF4W_7noWXFZAfHkxZsRGC9Xs", "use": "sig", "x": "…", "y": "…" } ] },
  "proofs": [ "eyJ0eXAiOiJkcG9wK2p3dC…signature" ],
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type":   "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
}
```

La PGD, a seguito della ricezione della richiesta, DEVE:

- verificare che siano presenti tutti i parametri obbligatori;
- verificare che l'entity_id corrisponda a un IdP registrato presso la PGD con stato active;
- verificare la corretta autenticazione dell'IdP secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP" (sottosezione "Processo di Verifica della PGD");
- validare il contenuto dell'array proofs utilizzando le relative chiavi presenti nel membro keys del JWK Set jwks, rifiutando la richiesta se anche una sola chiave dichiarata risulta priva di prova valida;
- verificare che nessuno dei kid dichiarati nel membro keys del JWK Set jwks risulti già registrato per l'IdP, rifiutando la richiesta in caso contrario.

Se tutte le verifiche hanno esito positivo, la PGD DEVE aggiungere le chiavi al materiale crittografico registrato, registrare un evento di audit (a titolo esemplificativo: entity_id, kid aggiunti, timestamp, IP source), inviare una notifica all'indirizzo e-mail registrato e fornire una risposta HTTP con status code 200 e Content-Type application/json, contenente i seguenti parametri:

- entity_id: [OBBLIGATORIO]. Stringa. DEVE corrispondere all'entity_id fornito nella richiesta;
- added_kids: [OBBLIGATORIO]. Array di stringhe. Elenco dei kid aggiunti con la presente richiesta;
- kids: [OBBLIGATORIO]. Array di stringhe. Elenco completo dei kid registrati per l'IdP al termine dell'operazione;
- updated_at: [OBBLIGATORIO]. Stringa. Data e ora dell'operazione. Formato: ISO 8601 UTC.

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "entity_id": "https://idp.example.it",
 "added_kids": ["NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xsidp-sig-2026-02"],
 "kids":        ["NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xsidp-sig-2026-01",
"NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs"],
 "updated_at": "2026-07-14T12:15:30Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Rimozione di Chiavi

La richiesta HTTP di rimozione di una o più chiavi DEVE essere inviata all'endpoint /pgd/idp/keys/remove usando il metodo POST. La rimozione ha effetto immediato.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “application/json”.

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP;
- kids: [OBBLIGATORIO]. Array di stringhe. Elenco dei kid delle chiavi da rimuovere;
- reason: [OPZIONALE]. Stringa. Motivazione della rimozione. Valori ammessi: compromised, superseded, unspecified;
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
POST /pgd/idp/keys/remove HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "kids": [ "NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs" ],
  "reason": "compromised",
  "client_assertion": "…",
  "client_assertion_type": "…"
}
```

La PGD, a seguito della ricezione della richiesta, DEVE:

- verificare che siano presenti tutti i parametri obbligatori;
- verificare che l'entity_id corrisponda a un IdP registrato presso la PGD;
- verificare la corretta autenticazione dell'IdP secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP";
- verificare che tutti i kid indicati risultino registrati per l'IdP.

La PGD NON DEVE consentire la rimozione di tutte le chiavi registrate: qualora l'operazione lasciasse l'IdP privo di materiale crittografico, la PGD DEVE rifiutare la richiesta con un errore, poiché l'IdP risulterebbe non operativo. In tal caso l'IdP DEVE aggiungere preventivamente una nuova chiave, oppure utilizzare l'endpoint di offboarding.

Se tutte le verifiche hanno esito positivo, la PGD DEVE rimuovere immediatamente le chiavi indicate dal materiale crittografico registrato, rifiutare da quel momento ogni JWT firmato con i kid rimossi, registrare

un evento di audit, inviare una notifica all'indirizzo e-mail registrato e fornire una risposta HTTP con status code 200 e Content-Type application/json, contenente i seguenti parametri:

- entity_id: [OBBLIGATORIO]. Stringa. DEVE corrispondere all'entity_id fornito nella richiesta;
- removed_kids: [OBBLIGATORIO]. Array di stringhe. Elenco dei kid rimossi con la presente richiesta;
- kids: [OBBLIGATORIO]. Array di stringhe. Elenco completo dei kid registrati per l'IdP al termine dell'operazione;
- removed_at: [OBBLIGATORIO]. Stringa. Data e ora dell'operazione. Formato: ISO 8601 UTC.

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

La PGD PUÒ rimuovere unilateralmente una o più chiavi di un IdP a fronte di evidenze di compromissione o di segnalazioni delle fonti autoritative. In tal caso la PGD DEVE notificare l'IdP tramite l'indirizzo e-mail registrato, secondo quanto previsto dalla sezione "Meccanismi di informazione tra soggetti".

Rotazione e Revoca delle Chiavi

La PGD non espone endpoint dedicati alla rotazione o alla revoca di una chiave: entrambe le operazioni si realizzano componendo le primitive di aggiunta e di rimozione descritte nelle sezioni precedenti.

L'IdP DEVE aggiungere la nuova chiave tramite POST /pgd/idp/keys e, una volta completata la transizione dei propri sistemi sulla nuova chiave, rimuovere quella precedente tramite POST /pgd/idp/keys/remove. Nel periodo intercorrente tra le due operazioni entrambe le chiavi risultano registrate e la PGD DEVE accettare come valide le firme prodotte con ciascuna di esse. È RACCOMANDATO che il periodo di sovrapposizione sia limitato al tempo strettamente necessario alla propagazione della nuova chiave sui sistemi dell'IdP.

In caso di compromissione l'IdP DEVE rimuovere immediatamente la chiave interessata tramite ~~DELETE~~ POST /pgd/idp/keys/remove, valorizzando il parametro reason con compromised e senza prevedere alcun periodo di sovrapposizione. Qualora la chiave compromessa sia l'unica registrata, l'IdP DEVE prima aggiungere una nuova chiave tramite POST /pgd/idp/keys e rimuovere successivamente quella compromessa tramite POST /pgd/idp/keys/remove, così da non interrompere la propria operatività.

Endpoint di Offboarding dell'IdP

La richiesta HTTP di offboarding DEVE essere inviata all'endpoint /pgd/idp/offboarding usando il metodo POST. Questo endpoint consente all'IdP di richiedere volontariamente la cessazione della propria abilitazione presso la PGD.

HTTP Request Headers:

- **Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "application/json".**

HTTP Request Body:

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP;
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dall'IdP, conforme a quanto definito nella sezione "Meccanismo di Autenticazione del SP" (applicato all'IdP);
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
POST /pgd/idp/offboarding HTTP/1.1
Host: pgd.example.it
Content-Type: application/json

{
  "entity_id": "https://idp.example.it",
  "client_assertion": "eyJhbGciOiJFUzI1Ni…signature",
  "client_assertion_type":   "urn:ietf:params:oauth:client-assertion-type:jwt-
bearer"
}
```

La PGD, a seguito della ricezione della richiesta, DEVE verificare l'autenticazione dell'IdP secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP" e che l'entity_id corrisponda a un IdP attualmente registrato.

Se tutte le verifiche hanno esito positivo, la PGD DEVE portare l'IdP nello stato offboarded, rimuovere l'intero materiale crittografico registrato, registrare un evento di audit (a titolo esemplificativo: entity_id, timestamp, IP source) e fornire una risposta HTTP con status code 200 e Content-Type application/json, contenente i seguenti parametri:

- status: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "offboarded";
- entity_id: [OBBLIGATORIO]. Stringa. DEVE corrispondere all'entity_id fornito nella richiesta;
- offboarding_date: [OBBLIGATORIO]. Stringa. Data e ora dell'offboarding. Formato: ISO 8601 UTC.

A valle dell'offboarding la PGD DEVE rifiutare ogni successiva richiesta proveniente dall'IdP verso gli endpoint IdP-PGD. L'IdP PUÒ richiedere un nuovo onboarding in qualsiasi momento, ripetendo l'intera procedura definita nella sezione "Endpoint di Onboarding dell'IdP".

La PGD PUÒ revocare unilateralmente l'abilitazione di un IdP, ad esempio per cessazione dei requisiti di accreditamento presso la fonte autoritativa. In tal caso la PGD DEVE notificare l'IdP tramite l'indirizzo e-mail registrato.

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Protocollo di scambio tra IdP e PGD

In questa sezione viene descritto il flusso tecnico di interazione e scambio dati tra l'IdP e la PGD. Tale protocollo si basa sul framework OAuth 2.0 e, in particolare, prevede l'utilizzo delle seguenti specifiche tecniche di riferimento e standard:

- The OAuth 2.0 Authorization Framework [RFC6749];
- Proof Key for Code Exchange (PKCE) [RFC7636];
- Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC7521];
- OAuth 2.0 Pushed Authorization Requests (PAR) [RFC9126];
- OAuth 2.0 Rich Authorization Requests (RAR) [RFC9396];
- The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR) [RFC9101];
- OAuth 2.0 Authorization Server Issuer Identification [RFC9207];
- OAuth 2.0 Demonstrating Proof of Possession (DPoP) [RFC9449];
- JSON Web Key (JWK) Thumbprint [RFC7638];
- **JSON Web Key (JWK) [RFC7517].**

Per garantire l'integrità e confidenzialità della comunicazione tra PGD e IdP è RICHIESTO l'utilizzo di chiavi di firma in accordo alla Sezione "Algoritmi Supportati" presenti in questo documento.
Per garantire l'integrità e confidenzialità della comunicazione tra PGD e IdP si RACCOMANDA in ogni caso l'utilizzo di chiavi di firma ad hoc, non già utilizzate per altre finalità.
In tutte le comunicazioni tra le parti, DEVE essere utilizzato il protocollo TLS nella versione 1.2 o superiore. L'utilizzo di versioni precedenti del protocollo TLS o del protocollo SSL è espressamente vietato.

Il diagramma di seguito riportato descrive il dettaglio del protocollo di scambio.

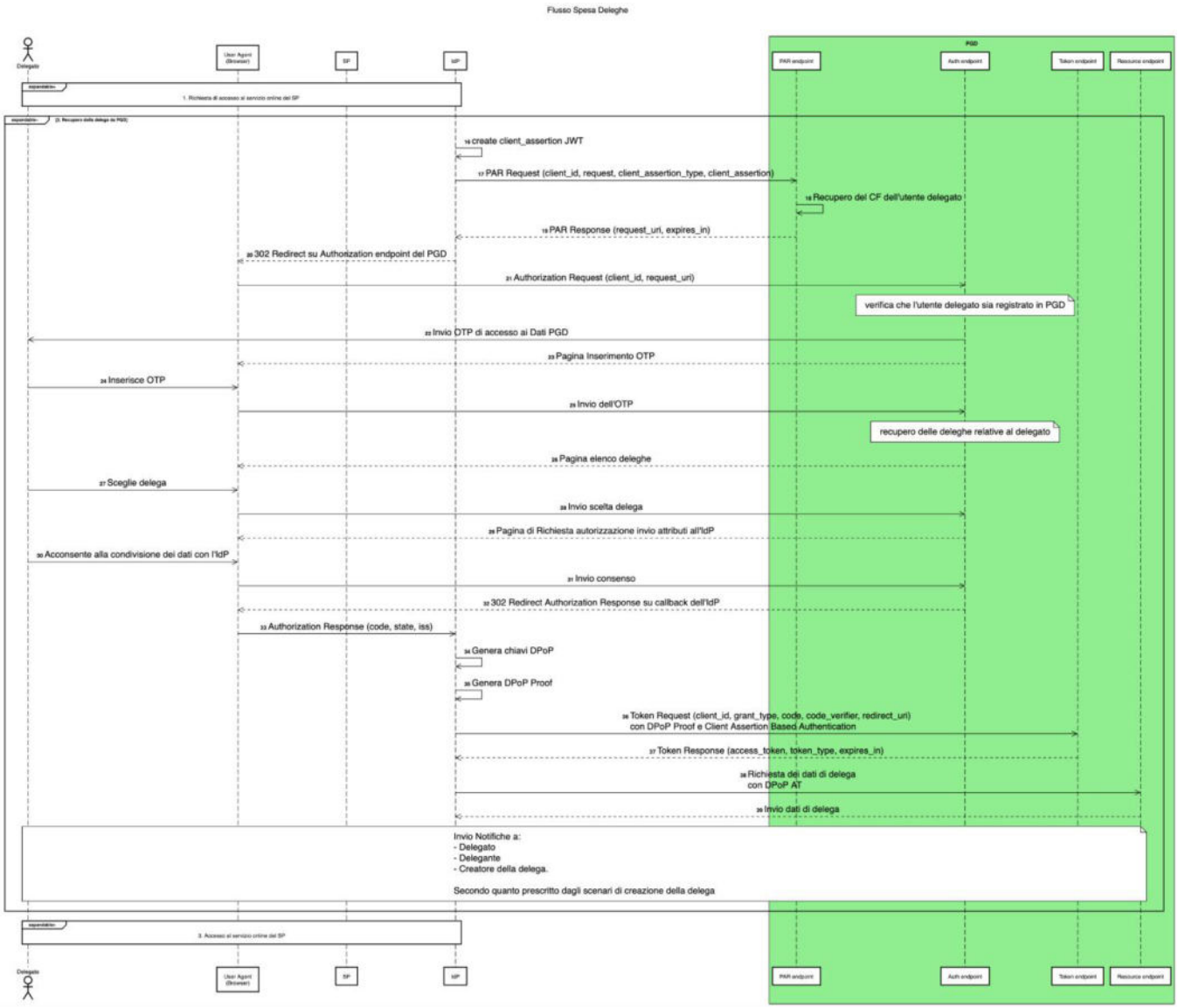


Figura 4 Protocollo di scambio tra IdP e PGD.

Nel diagramma sopra riportato, gli step da 1 a 16 descrivono la fase di richiesta di accesso ai servizi online del SP durante il protocollo di scambio tra SP e IdP (vedi sezione "Protocollo di scambio tra SP e IdP"**).**

Segue la descrizione dei passi, a partire dallo step 16, che compongono questa porzione del flusso.

Step 16: L'IdP crea un JWT "**$clientAssertion**" (contenente informazioni come il Codice Fiscale del delegato e altri dettagli volti a garantire l'autenticità della richiesta di accesso alla PGD da parte dell'IdP).

Step 17: L'IdP invia una richiesta al PAR endpoint della PGD con le informazioni necessarie.

A seguito della ricezione della richiesta di PAR da parte dell'IdP, la PGD DEVE verificare:

- la validità e le firme della "**$clientAssertion**" e del "**$responseObjec**t" inviati dall'IdP;
- la validità e le firme dell'authorization request originale (service_authorization_request) ed estrae i dati identificativi del cittadino e del SP da utilizzare nel flusso di accesso ai dati delle deleghe;
- la presenza del SP all'interno del registro dei SP abilitati alla PGD;
- la corrispondenza tra i parametri nel JWT e quelli nella richiesta HTTP il binding tra Request Object e client assertion attraverso il "client_id".

La PGD DEVE inoltre verificare l'unicità del parametro "**jti**", la validità temporale della richiesta e la conformità dei campi "**iss**", "**sub**" e "**aud**".
La PGD DEVE estrarre e verificare il contenuto di "**authorization_details**".
La PGD DEVE verificare che il CF contenuto dal parametro "**identifier**" corrisponda ad un CF precedentemente registrato in PGD.
La PGD DEVE verificare i parametri **scope** e **claims**, per restituire all'IdP i soli dati del delegante e delegato richiesti e disponibili. Qualora i campi siano assenti la PGD DEVE restituire il minimum dataset eIDAS.
In caso le precedenti verifiche non vadano tutte a buon fine, la PAR deve fallire e la PGD DEVE rispondere con un errore. L'IdP DEVE presentare all'utente un'apposita schermata di errore che lo informa dell'esito della richiesta. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 18: la PGD recupera il Codice Fiscale del delegato.

Step 19: la PGD risponde alla PAR con un "**request_uri**" valido per un tempo ridotto che consente di effettuare una Authentication Request.

Step 20: L'IdP reindirizza il browser all'endpoint di autorizzazione della PGD.

Step 21: Il browser invia la richiesta di autorizzazione al PGD (inclusi **client_id** e **request_uri**).

Alla ricezione della richiesta la PGD DEVE verificare la validità della "**request_uri**" della richiesta e recupera i dati relativi al Codice Fiscale del delegato precedentemente salvati in sessione.
Successivamente la PGD verifica che l'utente (Delegato) sia registrato nel sistema.

In caso di fallimento della PAR, la PGD DEVE rispondere con un errore. L'IdP DEVE presentare all'utente un'apposita schermata di errore che lo informa dell'esito della richiesta. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 22: La PGD invia un OTP al Delegato per consentirgli l'accesso ai dati delle deleghe.

L'OTP DEVE essere generato randomicamente, alfanumerico, lungo almeno sei caratteri ed essere inviato sulla e-mail certificata del Delegato raccolta durante il processo di creazione o accettazione della delega. Tale OTP DEVE avere durata non superiore a due minuti ed essere utilizzabile per un solo tentativo di accesso. Nell'ambito della stessa sessione di autenticazione e alla scadenza di un OTP, la PGD DEVE consentire all'utente di effettuare una sola nuova richiesta di OTP. Inoltre, PGD DEVE implementare meccanismi di rate limiting sulla generazione dell'OTP per codice fiscale e indirizzo IP con lockout temporaneo di un'ora dopo un numero massimo di 10 tentativi e registrare l'evento per analisi di sicurezza.

La PGD DEVE inoltre implementare logging e monitoring per rilevare pattern di attacco (es. richieste massive, tentativi distribuiti).

La mail contenente l'OTP DEVE mostrare l'informazione relativa al SP.

Step 23: La PGD mostra la pagina di inserimento dell'OTP.

La schermata di inserimento DEVE mostrare l'informazione relativa al nome del SP.

Step 24: Il delegato inserisce l'OTP.

Step 25: Il browser invia l'OTP alla PGD che ne verifica la validità.

La PGD DEVE verificare la correttezza dell'OTP e recupera le deleghe a lui associate (se presenti) e ne restituisce l'elenco al browser.

In caso di errato inserimento dell'OTP da parte dell'utente, la PGD DEVE mostrare una pagina di errore e DEVE consentire all'utente di richiedere un nuovo OTP. La PGD DEVE consentire al più due richieste di OTP nell'ambito della medesima sessione di autenticazione.

Nel caso in cui l'OTP inserito dall'utente sia correttamente validato dalla PGD, quest'ultima DEVE effettuare le verifiche di validità della delega in accordo con lo scenario di creazione della delega scelta, secondo quanto prescritto dal DCPM DELEGHE e dal relativo allegato tecnico.

In caso di fallimento dell'ultimo tentativo di inserimento dell'OTP da parte dell'utente, o delle verifiche di validità della delega, la PGD DEVE restituire una risposta di errore all'IdP mostrando all'utente una pagina di errore. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 26: La PGD mostra la pagina di scelta delle deleghe.

Step 27: Il Delegato sceglie una delega specifica sulla PGD.

La PGD DEVE consentire di annullare il flusso di accesso con delega in qualsiasi momento, per contemplare, ad esempio, il caso in cui l'utente non trovi nella lista delle deleghe disponibili quella che intendeva utilizzare.

Step 28: Il browser invia la scelta della delega al PGD.

Step 29: la PGD chiede all'utente (Delegato) l'autorizzazione ad inviare gli attributi all'IdP.

In caso di mancata autorizzazione, la PGD DEVE restituire una risposta di errore all'IdP mostrando all'utente una pagina di errore. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 30: L'utente (Delegato) autorizza la condivisione dei dati.

Step 31: Il browser invia l'autorizzazione al PGD.

Step 32: la PGD reindirizza il browser all'IdP con il codice di autorizzazione.

Step 33: Il Browser effettua la richiesta di autorizzazione all'IdP.

Step 34: L'IdP genera delle chiavi asimmetriche effimere.

Step 35: L'IdP genera una prova DPoP con le chiavi effimere appena create.

Step 36: L'IdP richiede un token all'endpoint **/token** della PGD inviando, con un'apposita richiesta contenente nell'HTTP Header DPoP, la prova DPoP alla PGD.

Alla ricezione della richiesta, la PGD DEVE validare la DPoP Proof:

- Verificandone la firma usando la chiave JWK nell'header;
- Validando il tipo "dpop+jwt". La PGD DEVE implementare una cache dei jti già utilizzati, con TTL pari alla massima validità della DPoP Proof, e DEVE rifiutare una richiesta il cui jti risulti già presente.
- Verificando l'unicità del jti;
- Verificando che htm e htu corrispondano alle specifiche del **/token** endpoint;
- Verificando la validità temporale della richiesta;
- Verificando il "**code_verifier**" rispetto alla "**code_challenge**" originale;
- Verificando che il redirect_uri corrisponda a quello della richiesta originale e che corrisponda a uno dei redirect_uris registrati per l'IdP;
- Verificando che la chiave usata per il DPoP Proof sia la stessa usata in precedenza.

La PGD DEVE rifiutare la DPoP proof il cui iat sia anteriore a 60 secondi rispetto al momento della ricezione.

La PGD DEVE, inoltre, memorizzare il thumbprint della chiave JWK e creare il Binding del thumbprint con l'access token generato.

Step 37: la PGD risponde con un "**access_token**".

La PGD NON DEVE MAI includere refresh token nella risposta, onde evitare che possa essere prolungata una sessione precedente per ri-ottenere i dati di una delega.

Step 38: L'IdP richiede i dati della delega al PGD usando il token ottenuto.

Step 39: la PGD invia i dati della delega (in particolare invia i dati del minimum dataset eIDAS del delegante in chiaro).

La PGD deve inoltre mandare l'informazione relativa al nome del SP nelle e-mail di notifica di accesso ai dati delle deleghe.

Le specifiche di UX/UI non sono definite all'interno di questa specifica.

Endpoint IdP-PGD

La PGD DEVE esporre i seguenti endpoint HTTP:

Endpoint	**Metodo**	**Descrizione**	**Autenticazione**
/pgd/registry	GET	Recupero del registro degli SP abilitati	Nessuna (da valutare se usare MTLS con IdP)
/as/par	POST	Pushed Authorization Request	Client Assertion
/authorize	GET	Authorization Request	Nessuna (session-based)
/token	POST	Token Request	Client Assertion + DPoP
/get-delegation-data	GET	Recupero dati delega	DPoP Access Token
/pgd/idp/onboarding	POST	Onboarding dell'IdP e registrazione del materiale crittografico e dei contatti	Client Assertion
/pgd/idp/status	POST	Verifica stato abilitazione e chiavi registrate dell'IdP	Client Assertion
/pgd/idp/contact	PUT	Modifica dei contatti dell'IdP	Client Assertion
/pgd/idp/keys	POST	Aggiunta di chiavi al materiale crittografico dell'IdP	Client Assertion

Endpoint	Metodo	Descrizione	Autenticazione
/pgd/idp/keys/remove	POST	Rimozione di chiavi dal materiale crittografico dell'IdP	Client Assertion
/pgd/idp/offboarding	POST	Offboarding dell'IdP	Client Assertion

Tutti gli endpoint DEVONO essere esposti tramite protocollo HTTPS (TLS 1.2 o superiore).

Gli endpoint di onboarding e gestione del ciclo di vita degli IdP (/pgd/idp/*) sono definiti nella sezione "Onboarding e integrazione dell'IdP con la PGD".

Endpoint del Registro

La PGD DEVE esporre un endpoint pubblico (/pgd/registry) per la distribuzione del registro degli SP abilitati.

Richiesta HTTP

La richiesta HTTP di download del Registro JWT DEVE essere inviata all'endpoint /pgd/registry usando il metodo GET, come riportato nel seguente esempio non normativo.

```
GET /pgd/registry HTTP/1.1
Host: pgd.example.it
Accept: application/jwt
```

Risposta HTTP

A seguito di una richiesta HTTP, la PGD DEVE:

- Calcolare dinamicamente il valore max-age dell'header Cache-Control come exp - tempo_corrente**;**
- inviare nel body dell'HTTP Response un JWT in formato compatto, firmato dalla PGD e che rappresenta il registro degli SP abilitati.

L'HTTP Response Headers DEVE contenere i seguenti parametri:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**application/jwt**"**;**
- **Cache-Control**: [OBBLIGATORIO]. DEVE contenere la direttiva max-age con valore dinamico calcolato come max-age = exp - tempo_corrente dove exp è il claim di scadenza del JWT

e tempo_corrente è il timestamp UNIX al momento della generazione della risposta HTTP. Esempio: Cache-Control: max-age=86400**;**

- **Last-Modified**: [OBBLIGATORIO]. Stringa. Data e ora dell'ultima modifica del Registro JWT (timestamp di generazione)**.**

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/jwt
Cache-Control: max-age=86400
Date: Fri, 17 Jan 2026 12:00:00 GMT
Last-Modified: Fri, 17 Jan 2026 00:00:05 GMT

eyJhbGciOiJFUzI1NiIsInR5cCI6InBnZC1yZWdpc3RyeStqd3QiLCJraWQiOiIzZjIzMWI5OS1mN
mQ2LTQ1MTgtMDdiOS0wOGQwOTEzZmQyOGQifQ.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJ
pYXQiOjE3MzQ5NjAwMDAsImV4cCI6MTczNTA0NjQwMCwic2FtbF9lbnRpdHlfaWRzIjpbImh0dHBz
Oi8vc3AxLmV4YW1wbGUub3JnIiwiaHR0cHM6Ly9zcDMuZ292Lml0L3NlcnZpY2VzL2RlbGVnaGUiX
Swib2lkY19jbGllbnRfaWRzIjpbImh0dHBzOi8vc3AyLmV4YW1wbGUuZ292Lml0Il19.MEYCIQCa1
b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2wIwQHx3y4z5a6b7c8d9e0f1g2h3i4j5k6l7
m8n9o0p1q2r3s4t5u6
```

Il formato del Registro JWT è definito nella sezione “Formato del Registro JWT”.

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Verifiche dell’IdP

Gli IdP che consumano questo endpoint DEVONO:

1. **Implementare refresh proattivo**: Gli IdP DEVONO implementare un meccanismo di refresh proattivo che scarica il Registro JWT dalla PGD prima della scadenza (exp), evitando latenze durante l'autenticazione degli utenti e gestendo eventuali indisponibilità temporanee della PGD. Il refresh proattivo consente di mantenere sempre in cache un registro valido.

2. **Fallback a refresh sincrono**: In caso di mancato refresh proattivo (es. primo avvio, scadenza registro, failure dello scheduler), l'IdP PUÒ effettuare un refresh sincrono durante il flusso di autenticazione, ma questo approccio NON DOVREBBE essere implementato in produzione per evitare latenze user-facing. In caso di fallimento del refresh sincrono, l’IdP NON DEVE fornire all’utente l’opzione di accesso con delega.

3. **Verificare la firma del JWT**: Prima di utilizzare il contenuto del registro, l'IdP DEVE verificare la firma del JWT utilizzando la chiave pubblica della PGD distribuita secondo quanto specificato nella sezione "Distribuzione Chiave Pubblica PGD".

4. **Verificare la validità temporale**: L'IdP DEVE verificare che il JWT non sia scaduto controllando il claim exp.

5. **Rispettare Cache-Control**: L'IdP DEVE rispettare l'header Cache-Control fornito dalla PGD e memorizzare in cache il Registro JWT per una durata NON superiore a max-age e NON superiore alla scadenza JWT (exp).

6. **Verifica abilitazione SP**: Durante il flusso di autenticazione, l'IdP DEVE verificare la presenza, nell'array service_providers, di un oggetto con entity_id corrispondente e protocol coerente con il protocollo di autenticazione in uso. Solo se l'identificativo è presente e il JWT è valido, l'IdP PUÒ offrire l'opzione di autenticazione con delega**.**

Quando la PGD revoca un SP (revoca amministrativa o offboarding), l'oggetto corrispondente alla tripla del SP viene rimosso dall'array service_providers. La revoca diventa effettiva presso gli IdP entro massimo 24 ore (al prossimo refresh proattivo o sincrono). La frequenza di generazione del Registro JWT da parte della PGD PUÒ essere inferiore a 24 ore per garantire propagazione più rapida delle revoche.

Client Authentication

A garanzia della sicurezza delle comunicazioni, l'IdP DEVE autenticarsi all'Authorization Server della PGD secondo le specifiche descritte in Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC7521].

Il sistema DEVE quindi, implementare un meccanismo di autenticazione di Client Authentication che prevede la generazione di una assertion in formato JWT (**$clientAssertion**) firmata dall'IdP (il Client) e verificata dall'Authorization Server della PGD.

Tale assertion attesta l'identità del client (**l'**IdP) e viene trasmessa come parte della richiesta HTTP. La client authentication basata su JWT DEVE essere utilizzata sia per le richieste verso il PAR endpoint che per quelle dirette al Token endpoint della PGD e nei seguenti paragrafi ne viene presentata la specifica.

La PGD DEVE verificare la firma della $clientAssertion utilizzando esclusivamente le chiavi pubbliche dell'IdP registrate presso la PGD in fase di onboarding e, eventualmente, aggiornate tramite gli endpoint di gestione del materiale crittografico.

Il Client Assertion JWT **($clientAssertion**) DEVE contenere i seguenti campi:

Parametri dell'header:

- **typ: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "pgd-client-assertion+jwt";**
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [CONDIZIONALE]. **OBBLIGATORIO se non è presente il parametro x5c. Stringa. DEVE contenere il kid della chiave pubblica dell'IdP registrata presso la PGD, valorizzato con il JWK thumbprint [RFC7638] come previsto per il materiale crittografico IdP-PGD**;
- **x5c**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **kid**. Stringa. DEVE contenere il certificato x.509 relativo alla chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo univoco URL HTTPS dell'IdP richiedente;
- **sub**: [OBBLIGATORIO]. Stringa. Identificativo univoco URL HTTPS dell'IdP richiedente;
- **nbf**: [OBBLIGATORIO]. Intero. Timestamp Unix che indica il momento di inizio validità del token;
- **exp**: [OBBLIGATORIO]. Intero. Timestamp Unix che indica il momento di scadenza del token;
- **aud**: [OBBLIGATORIO]. Stringa. URL dell'endpoint Authorization della PGD;
- **jti**: [OBBLIGATORIO]. Stringa. Identificativo univoco del JWT in formato UUID v4 per prevenire replay attacks;
- **session_id**: [OPZIONALE]. Stringa. Identificativo di sessione.

Di seguito, un esempio non normativo di "$**clientAssertion**":

```
{
      "typ": "pgd-client-assertion+jwt",
      "alg": "ES256",
      "kid": "cde6a4c1-3032-4a64-be15-18973dc3ad9e"
}
.
{
      "iss": "https://idp.example.it",
      "sub": "https://idp.example.it",
      "nbf": 1734960000,
      "exp": 1734960300,
      "aud": "https://pgd.example.it/auth",
      "jti": "e958c478-0b58-4dfa-a89b-87b317acc5f1"
}
```

PAR Endpoint

Il PAR endpoint DEVE:

- essere protetto dal meccanismo di client authentication come definito nella Sezione "Client Authentication";
- utilizzare il parametro **request** come definito in JAR [RFC9101] per inviare il Request JWT Object all'Authorization Server di PGD;
- utilizzare il parametro **authorization_details** come definito in RAR [RFC9396] per veicolare l'identificativo dell'utente delegato per il quale si richiedono le informazioni di delega.

PAR Request

La richiesta PAR (Pushed Authentication Request) DEVE usare il metodo POST.

La HTTP Request DEVE contenere il seguente HTTP Header:

- **Content-type**: [OBBLIGATORIO]. Stringa. Valorizzato con "**application/x-www-form-urlencoded**".

La HTTP Request DEVE contenere i seguenti query parameters:

- **client_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP registrato presso la PGD in formato HTTPS URL;

- **state**: [OBBLIGATORIO]. Stringa casuale di lunghezza minima 32 caratteri che DEVE essere inclusa nelle successive risposte per prevenire attacchi di tipo CSRF;
- **request**: [OBBLIGATORIO]. Stringa. DEVE contenere un JWT **$requestObject**;
- **client_assertion_type**: [OBBLIGATORIO]. DEVE essere valorizzato con la stringa "urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer";
- **client_assertion**: [OBBLIGATORIO]. DEVE contenere un JWT firmato dall'IdP contenente le informazioni di autenticazione (**$clientAssertion**).

Di seguito, un esempio non normativo della richiesta:

```
POST /as/par HTTP/1.1
Host: pgd.example.it
Content-Type: application/x-www-form-urlencoded

&client_id=https%3A%2F%2Fidp.example.it
&state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
&request=$requestObject
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
&client_assertion=$clientAssertion
```

La PAR Request DEVE contenere un JWT firmato ($requestObject) con i seguenti campi:

Parametri dell'header:

- **typ:** [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**oauth-authz-req+jwt**";
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro x5c. Stringa. DEVE contenere il kid della chiave pubblica dell'IdP registrata presso la PGD, valorizzato con il JWK thumbprint [RFC7638] come previsto per il materiale crittografico IdP-PGD;
- **x5c**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **kid**. Stringa. DEVE contenere il certificato x.509 relativo alla chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT.

Parametri del payload:

- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL dell'endpoint PAR della PGD;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **response_type**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**code**";
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP registrato presso la PGD;
- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL HTTPS dell'Identity Provider che ha emesso il token;
- **state**: [OBBLIGATORIO]. Stringa. DEVE contenere un valore opaco per mantenere lo stato tra la richiesta e il callback;

- **scope**: [OPZIONALE]. Stringa. DEVE essere valorizzato come definito nella sezione "Costruzione dei parametri claims e scope";
- **claims:** [OPZIONALE]. JSON Object. DEVE contenere gli attributi del delegante e del delegato richiesti dal SP, secondo quanto definito nella sezione "Costruzione dei parametri claims e scope";
- **code_challenge**: [OBBLIGATORIO]. Stringa. DEVE contenere il challenge PKCE codificato in BASE64URL;
- **code_challenge_method**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**S256**". L'IdP DEVE quindi supportare lo specifico algoritmo;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. L'Array DEVE contenere almeno un oggetto JSON contenente i seguenti parametri:
    - **type**: [OBBLIGATORIO]. Stringa. Il parametro DEVE essere valorizzato con la stringa **delegation_record**;
    - **identifier**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'utente delegato valorizzato con il codice fiscale dell'utente;
    - **service_authorization_request**: [OBBLIGATORIO]. Stringa BASE64. Richiesta di autorizzazione originaria fatta dal SP all'IdP, che attesta l'effettiva richiesta di accesso al servizio da parte di un utente. Per SAML il valore DEVE contenere l'elemento <samlp:AuthnRequest> inviato dal SP all'IdP; per OIDC DEVE contenere il Request Object JWT dell'Authentication Request. In entrambi i casi il contenuto è codificato in BASE64. La PGD DEVE verificarne la firma secondo le regole tecniche del protocollo di riferimento**;**
    - **service_protocol**: [OBBLIGATORIO]: Stringa. Protocollo utilizzato dal SP nell'ambito delle federazioni CIE/SPID. Valori ammessi: saml, oidc;
    - **locations**: [OBBLIGATORIO]. Array di stringhe. l'Array DEVE contenere almeno una stringa valorizzata con il Resource endpoint di PGD;
    - **redirect_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL a cui la PGD DEVE reindirizzare dopo il completamento del flusso. La PGD DEVE verificare che il redirect_uri presente nella richiesta corrisponda a uno dei redirect_uris registrati per l'IdP. Richieste con un redirect_uri non registrato DEVONO essere rifiutate.

Segue un esempio non normativo del $**requestObject**:


```
{
      "typ": "oauth-authz-req+jwt",
      "alg": "ES256",
      "kid": "cde6a4c1-3032-4a64-be15-18973dc3ad9e"
}
.
{
      "jti": "f8555ceb-c65c-4025-9378-b6672b6149af",
      "aud": "https://pgd.example.it/par",
      "iat": 1734960000,
      "exp": 1734960300,
      "response_type": "code",
      "client_id": "https://idp.example.it",
      "iss": "https://idp.example.it",
      "state": "fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd",
      "code_challenge": "E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-cM",
      "code_challenge_method": "S256",
```

```
      "redirect_uri": "https://idp.example.com/cb",
      "authorization_details": [
            {
                  "type": "delegation_record",
                  "identifier": "MROXXXXXXXXXXXXX",
                  "service_authorization_request": "…",
                  "service_protocol": "oidc",
                  "locations":      ["https://pgd.example.it/get-delegation-
            data"]
            }
      ]
}
```

Costruzione dei parametri claims e scope

Il parametro claims veicola verso la PGD gli attributi del delegante e del delegato richiesti dal SP.
La PGD DEVE utilizzarlo esclusivamente come filtro sui dati restituiti nel JWT delegation_info.

L'oggetto claims DEVE utilizzare la sintassi definita da OpenID Connect Core, con le chiavi di primo livello id_token e/o userinfo.

In OIDC l'IdP NON DEVE modificare l'oggetto claims ricevuto dal SP e la PGD DEVE considerare l'unione dei claim presenti in entrambe le chiavi.
In SAML, l'oggetto claims DEVE essere costruito dall'IdP a partire dai RequestedAttribute dell'AttributeConsumingService individuato dall'AttributeConsumingServiceIndex indicato nella AuthnRequest del SP, e DEVE essere inviato utilizzando la sola chiave userinfo.

Per ciascun claim l'obbligatorietà dell'attributo DEVE seguire quanto richiesto dal SP.
In OIDC questo è garantito dal fatto che l'IdP invia alla PGD il parametro claims come ricevuto dal SP.
Per SAML l'IdP DEVE valorizzare il parametro essential a true per gli attributi con isRequired="true" e a false altrimenti.

I claim POSSONO essere espressi con gli identificativi utilizzati dal SP (claim OIDC/SPID o RequestedAttribute SAML). La PGD DEVE effettuare la corrispondenza tra tali identificativi e i nomi degli oggetti delegate e delegator definiti nella sezione "Resource Response". I claim non riconosciuti DEVONO essere ignorati.

Di seguito una tabella per la conversione dei nomi dei claim scambiati tra IdP-PGD e viceversa.

Claim OIDC richiesto dal SP	**Attributo SAML richiesto dal SP**	**Campo PGD in delegation_info**
given_name	name	name
family_name	familyName	family_name

birthdate	dateOfBirth	birthdate
email	email	email
https://attributes.eid.gov.it/fiscal_number	fiscalNumber	fiscal_number

Il parametro scope deve essere gestito come segue.
In OIDC l'IdP NON DEVE modificare il valore di scope ricevuto dal SP e DEVE riportarlo as-is nella richiesta verso la PGD.
In SAML il concetto di scope non è previsto per la richiesta di attributi: l'IdP NON DEVE utilizzare scope per veicolare gli attributi richiesti, che DEVONO essere espressi unicamente tramite claims costruito dai RequestedAttribute; il parametro scope DEVE pertanto essere omesso.

Gli attributi richiesti tramite il solo scope sono considerati essenziali (essential = true).

Qualora i parametri scope e claims siano assenti, la PGD DEVE restituire il minimum dataset eIDAS.

PAR Response

A seguito della verifica di correttezza della Request effettuata dall'IdP, il PAR endpoint DEVE inviare all'IdP una HTTP Response con HTTP Response Code valorizzato a 201 Created.

La HTTP Response DEVE contenere i seguenti HTTP Headers:

- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con "**no-cache, no-store**" per evitare che le informazioni contenute vengano mantenute in cache;
- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**application/json**".

Parametri nel body:

- **request_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere un identificativo univoco che fa riferimento alla richiesta di autorizzazione memorizzata. Il valore DEVE essere **urn:ietf:params:oauth:request_uri:<reference-value>**. Il valore di **reference-value** DEVE essere generato in modo random e non predicibile secondo quanto prescritto in Sezione 10.10 di RFC6749;
- **expires_in**: [OBBLIGATORIO]. Intero. DEVE indicare il tempo di validità in secondi della **request_uri** restituita.

Si riporta, di seguito, un esempio non normativo della risposta:

```
HTTP/1.1 201 Created
Cache-Control: no-cache, no-store
Content-Type: application/json

{
      "request_uri":  "urn:ietf:params:oauth:request_uri:bwc4JK-ESC0w8acc191e-
Y1LTC2",
      "expires_in": 60
}
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Authorization Endpoint

Authorization Request

A seguito dell'ottenimento della risposta all'endpoint PAR l'IdP utilizza l'OAuth 2.0 Authorization endpoint della PGD per inviare una Authorization Request. Questa DEVE includere come query parameters il **client_id** e la **request_uri** ottenuta dalla risposta del PAR endpoint.
La richiesta di Authorize DEVE usare il metodo GET.

La HTTP Request DEVE contenere i seguenti query parameters:

- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP registrato presso la PGD in formato URL HTTPS;
- **request_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco ricevuto nella risposta del PAR endpoint.

Di seguito, un esempio non normativo della richiesta:

```
GET
/authorize?client_id=https%3A%2F%2Fidp.example.it&request_uri=urn%3Aietf%3Apa
rams%3Aoauth%3Arequest_uri%3Abwc4JK-ESC0w8acc191e-Y1LTC2    HTTP/1.1    Host:
pgd.example.it
```

Authorization Response

L'Authorization Server DEVE reindirizzare lo User-Agent all'URL specificato nel parametro **redirect_ur**i della richiesta originale e aggiungere i seguenti parametri in URLencoded format:

- **code**: [OBBLIGATORIO]. Stringa. DEVE contenere l'authorization code generato dall'Authorization Server;
- **state**: [OBBLIGATORIO]. Stringa. DEVE contenere il valore esatto dello state ricevuto nella PAR Request;
- **iss**: [OBBLIGATORIO]. Stringa. Il valore DEVE contenere l'identificativo univoco della PGD e DEVE essere una stringa in formato HTTPS URL. L'utilizzo di questo parametro è richiesto per mitigare attacchi di tipi mix-up, come descritto in RFC9207.

Segue un esempio non normativo della risposta:

```
HTTP/1.1      302      Found      Location:      https://idp.example.it/cb?
code=SplxlOBeZQQYbYS6WxSbIA          &state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
&iss=https%3A%2F%2Fpgd.example.it
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Token Endpoint

Il Token endpoint DEVE essere protetto dal meccanismo di client authentication come definito nella Sezione "Client Authentication".
Il Token endpoint DEVE, inoltre, supportare l'utilizzo di Access Token DPoP, secondo quanto definito in RFC9449 e NON DEVE rilasciare Access Token di tipo diversi da DPoP Access Token.

DPoP Proof

La DPoP Proof DEVE essere generata dall'IdP e inviata nell'header della Token Request in fase di ottenimento del DPoP Access Token e della Resource Request per la richiesta e l'ottenimento della delega dell'utente.

Nella Token Request l'IdP DEVE generare la DPoP proof come definito di seguito.

Parametri dell'header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**dpop+jwt**";
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **jwk**: [OBBLIGATORIO]. Oggetto. DEVE contenere la chiave pubblica in formato JWK in accordo a quanto previsto in RFC7517 e RFC7518.

Parametri del payload:

- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **htm**: [OBBLIGATORIO]. Stringa. DEVE contenere il metodo HTTP della richiesta;
- **htu**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL completo dell'endpoint;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token.

Di seguito, un esempio non normativo della DPoP proof:

```
{
      "typ": "dpop+jwt",
      "alg": "ES256",
      "jwk":
      {
            "kty": "EC",
            "x": "l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
            "y": "9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA",
            "crv": "P-256"
      }
}
.
```

```
{
      "jti": "f6ec98f5-d78a-4fc8-8e9d-9346166a4d3e",
      "htm": "POST",
      "htu": "https://pgd.example.it/endpoint",
      "iat": 1734960000
}
```

Nell'utilizzo del DPoP Access Token, ovvero in fase di accesso al Resource endpoint, in aggiunta ai parametri sopra riportati, l'IdP DEVE aggiungere il seguente parametro alla DPoP Proof:

- **ath**: [OBBLIGATORIO]. Stringa. DEVE contenere l'hash SHA256 dell'**access_token** ottenuto dalla PGD.

Token Request

La richiesta del token DEVE essere chiamata tramite metodo HTTP POST e contenere i seguenti HTTP header:

- **Host**: [OBBLIGATORIO]. DEVE contenere l'hostname del server;
- **DPoP**: [OBBLIGATORIO]. DEVE contenere il DPoP Proof JWT;
- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**application/x-www-form-urlencoded**".

e parametri nel body:

- **grant_type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**authorization_code**";
- **code**: [OBBLIGATORIO]. DEVE contenere il codice di autorizzazione ricevuto;
- **code_verifier**: [OBBLIGATORIO]. DEVE contenere il **code_verifier** originale;
- **redirect_uri**: [OBBLIGATORIO]. DEVE corrispondere alla redirect_uri originale;
- **client_assertion_type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**urn:ietf:params:oauth:client-assertion-type:jwt-bearer**";
- **client_assertion**: [OBBLIGATORIO]. DEVE contenere il JWT di autenticazione del client.

Di seguito, un esempio non normativo della richiesta:

```
POST /token HTTP/1.1
Host: pgd.example.it
DPoP: eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrIjp7Imt0eSI6Ik\
VDIiwieCI6Imw4dEZyaHgtMzR0VjNoUklDUkRZOXpDa0RscEJoRjQyVVFVZldWQVdCR\
nMiLCJ5IjoiOVZFNGpmX09rX282NHpiVFRsY3VOSmFqSG10NnY5VERWclUwQ2R2R1JE\
QSIsImNydiI6IlAtMjU2In19.eyJqdGkiOiItQndDM0VTYzZhY2MybFRjIiwiaHRtIj\
oiUE9TVCIsImh0dSI6Imh0dHBzOi8vc2VydmVyLmV4YW1wbGUuY29tL3Rva2VuIiwia\
WF0IjoxNTYyMjYyNjE2fQ.2-GxA6T8lP4vfrg8v-FdWP0A0zdrj8igiMLvqRMUvwnQg\
4PtFLbdLXiOSsX0x7NVY-FNyJK70nfbV37xRZT3Lg
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=code&code_verifier=dBjftJeZ4CVP-
mB92K27uhbUJU1p1r_wW1gFWFOEjXk&redirect_uri=https%3A%2F%2Fidp.example.it%2Fcb
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer&client_assertion=$clientAssertion
```

Token Response

In caso le verifiche effettuate sulla Token Request abbiano tutte successo, la PGD DEVE rispondere con un HTTP code 200 ed i seguenti HTTP header:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**application/json;charset=UTF-8**";
- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con "**no-store**" per evitare che le informazioni contenute vengano mantenute in cache;
- **Pragma**: [OBBLIGATORIO]. DEVE essere valorizzato con "**no-cache**" per evitare che le informazioni contenute vengano mantenute in cache.

Il body della risposta DEVE contenere i campi:

- **access_token**: [OBBLIGATORIO]. Stringa. DEVE contenere il JWT;
- **token_type**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**DPoP**";
- **expires_in**: [OBBLIGATORIO]. Intero. DEVE indicare la durata del token in secondi;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. L'Array DEVE contenere almeno un oggetto JSON contenente i seguenti parametri:
    - **type**: [OBBLIGATORIO]. Stringa. Il parametro DEVE essere valorizzato con la stringa "**delegation_record**";
    - **identifier**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'utente delegato valorizzato con il codice fiscale dell'utente;
    - **service_authorization_request:** [OBBLIGATORIO]. Stringa BASE64. Richiesta di autorizzazione originaria fatta dal SP all'IdP codificata in BASE64, che attesta l'effettiva richiesta di accesso al servizio da parte di un utente;
    - ~~o~~ **service_protocol:** [OBBLIGATORIO]: Stringa. Protocollo utilizzato dal SP nell'ambito delle federazioni CIE/SPID. Valori ammessi: saml, oidc;
    - **locations**: [OBBLIGATORIO]. Array di stringhe. l'Array DEVE contenere almeno una stringa valorizzata con il Resource endpoint di PGD.

Di seguito, un esempio non normativo:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
      "access_token":
"ewogICAgInR5cCI6ICJhdCtqd3QiLAogICAgImFsZyI6ICJFUzI1NiIsCiAgICAia2lkIjogIjYw
MmZiYzNiLWExMTctNGE0NS1hNWQyLWM0YjhlZGRkMDQ4MiIKfS4KewogICAgImlzcyI6ICJodHRwc
zovL3BnZC5leGFtcGxlLm9yZyIsCiAgICAic3ViIjogImQ0ZTBiYjM4N2FhMjU1NmZmMzA2OTI1Zm
RmYjlhNzY1IiwKICAgICJhdWQiOiAiaHR0cHM6Ly9wZ2QuZXhhbXBsZS5vcmciLAogICAgImlhdCI
6IDE3MTU4NDI1NjAsCiAgICAiZXhwIjogMTc3ODkxNDU2MCwKICAgICJqdGkiOiAiZjk2NTVjZWIt
YzY1Yy00MDI1LTkzNzgtYjY2NzJiNjE0OWJnIiwKICAgICJjbGllbnRfaWQiOiAiaHR0cHM6Ly9pZ
HAuZXhhbXBsZS5vcmciLAogICAgImNuZiI6IHsKICAgICAgImprdCI6ICI5NTE1NzRhZWUxYmI3OT
A3YWUxZWMzMTA5ZGIyYjIyNSIKICAgIH0KfQo=",
```

```
      "token_type": "DPoP",
      "expires_in": 3600,
      "authorization_details": [
            {
                  "type": "delegation_record",
                  "identifier": "MROXXXXXXXXXXXXX",
                  "service_authorization_request": "…",
                  "service_protocol": "oidc",
                  "locations":      ["https://pgd.example.it/get-delegation-
            data"]
            }
      ]
}
```

Access Token

L'access_token DEVE essere un JWT con:

Parametri dell'header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**at+jwt**";
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave del PGD utilizzata per la verifica della firma del JWT. Il valore DEVE essere in formato UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della PGD in formato HTTPS URL;
- **sub**: [OBBLIGATORIO]. Stringa. DEVE contenere un identificativo univoco pairwise opaco dell'utente;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della PGD in formato HTTPS URL;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL dell'IdP;
- **cnf**: [OBBLIGATORIO]. Oggetto. DEVE contenere:
    - **jkt**: [OBBLIGATORIO]. Stringa. DEVE contenere l'hash della chiave pubblica JWK del DPoP;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. Il parametro DEVE essere valorizzato come riportato nella Token Response.

Di seguito, un esempio non normativo:

```
{
      "typ": "at+jwt",
      "alg": "ES256",
      "kid": "602fbc3b-a117-4a45-a5d2-c4b8eddd0482"
}
.
{
      "iss": "https://pgd.example.it",
      "sub": "d4e0bb387aa2556ff306925fdfb9a765",
      "aud": "https://pgd.example.it",
      "iat": 1734960000,
      "exp": 1734960600,
      "jti": "f9655ceb-c65c-4025-9378-b6672b6149bg",
      "client_id": "https://idp.example.it",
      "cnf":
      {
            "jkt": "951574aee1bb7907ae1ec3109db2b225"
      },
      "authorization_details": [
            {
                  "type": "delegation_record",
                  "identifier": "MROXXXXXXXXXXXXX",
                  "service_authorization_request": "…",
                  "service_protocol": "oidc",
                  "locations": [ "https://pgd.example.it/" ]
            }
      ]
}
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Get Delegation Data Endpoint

Get Delegation Data Request

La richiesta delle informazioni sulla delega DEVE essere effettuata all'endpoint **/get-delegation-data** con metodo HTTP GET ed i seguenti header HTTP:

- **Authorization**: [OBBLIGATORIO]. DEVE contenere il DPoP Access Token nel formato **DPoP {$accessToken}**;
- **DPoP**: [OBBLIGATORIO]. DEVE contenere il DPoP Proof JWT arricchito col campo **ath**, come descritto nella Sezione "DPoP Proof";

Il parametro **$accessToken** è un JWT che DEVE avere i seguenti campi

Parametri di header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**at+jwt**";

- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave utilizzata per la firma in UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL della PGD;
- **sub**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'utente;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL della PGD;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP in formato HTTPS URL;
- **cnf**: [OBBLIGATORIO]. Oggetto. DEVE contenere:
    - **jkt**: [OBBLIGATORIO]. Stringa. DEVE contenere il thumbprint della chiave DPoP.

Di seguito, un esempio non normativo della richiesta:

```
GET /get-delegation-data HTTP/1.1
Host: pgd.example.it
Authorization: DPoP
ewogICAgInR5cCI6ICJhdCtqd3QiLAogICAgImFsZyI6ICJFUzI1NiIsCiAgICAia2lkIjogIjYwM
mZiYzNiLWExMTctNGE0NS1hNWQyLWM0YjhlZGRkMDQ4MiIKfS4KewogICAgImlzcyI6ICJodHRwcz
ovL3BnZC5leGFtcGxlLm9yZyIsCiAgICAic3ViIjogImQ0ZTBiYjM4N2FhMjU1NmZmMzA2OTI1ZmR
mYjlhNzY1IiwKICAgICJhdWQiOiAiaHR0cHM6Ly9wZ2QuZXhhbXBsZS5vcmciLAogICAgImlhdCI6
IDE3MTU4NDI1NjAsCiAgICAiZXhwIjogMTc3ODkxNDU2MCwKICAgICJqdGkiOiAiZjk2NTVjZWItY
zY1Yy00MDI1LTkzNzgtYjY2NzJiNjE0OWJnIiwKICAgICJjbGllbnRfaWQiOiAiaHR0cHM6Ly9pZH
AuZXhhbXBsZS5vcmciLAogICAgImNuZiI6IHsKICAgICAgImprdCI6ICI5NTE1NzRhZWUxYmI3OTA
3YWUxZWMzMTA5ZGIyYjIyNSIKICAgIH0KfQo
DPoP:
eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrIjp7Imt0eSI6IkVDIiwieCI6Imw4d
EZyaHgtMzR0VjNoUklDUkRZOXpDa0RscEJoRjQyVVFVZldWQVdCRnMiLCJ5IjoiOVZFNGpmX09rX2
82NHpiVFRsY3VOSmFqSG10NnY5VERWclUwQ2R2R1JEQSIsImNydiI6IlAtMjU2In19.eyJqdGkiOi
ItQndDM0VTYzZhY2MybFRjIiwiaHRtIjoiUE9TVCIsImh0dSI6Imh0dHBzOi8vc2VydmVyLmV4YW1
wbGUuY29tL3Rva2VuIiwiaWF0IjoxNTYyMjYyNjE2fQ.2-GxA6T8lP4vfrg8v-
FdWP0A0zdrj8igiMLvqRMUvwnQg4PtFLbdLXiOSsX0x7NVY-FNyJK70nfbV37xRZT3Lg
```

Resource Response

In caso di esito delle verifiche positive, la PGD risponde con i dati della delega selezionata inseriti in un JWT.

La HTTP Response DEVE contenere i seguenti HTTP Header:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con "**application/json;charset=UTF-8**";

- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con "**no-store**" per evitare che le informazioni contenute vengano mantenute in cache;
- **Pragma**: [OBBLIGATORIO]. DEVE essere valorizzato con "**no-cache**" per evitare che le informazioni contenute vengano mantenute in cache.

Il body della risposta restituisce un JSON contenente nel parametro "**delegation_info**" che DEVE essere valorizzato con un JWT come definito di seguito:

Parametri di header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "**pgd-delegation-data-response+jwt**";
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave pubblica del PGD utilizzata per la verifica della firma del JWT. Il valore DEVE essere in formato UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo della PGD che ha emesso il JWT (es. https://pgd.example.it/);
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo dell'IdP destinatario del JWT (client_id dell'IdP che ha richiesto la risorsa);
- **version**: [OBBLIGATORIO]. Stringa. Contiene l'identificativo di versione della DelegationInfo;
- **delegate**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegato;
    - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegato;
    - **family_name**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegato;
    - **birthdate**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegato nel formato ISO 8601 (YYYY-MM-DD);
    - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo e-mail del delegato se disponibile;
    - **fiscal_number**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegato.
- **delegator**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegante;
    - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegante;
    - **family_name**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegante;
    - **birthdate**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegante nel formato ISO 8601 (YYYY-MM-DD);
    - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo e-mail del delegante se disponibile;
    - **fiscal_number**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegante.
- **delegation_type**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo del tipo di delega conferita al delegato *(vedere tab. 1)*;
- **delegation_created_at:** [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica la data di creazione della delega;
- **iat:** [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **nbf**: [OPZIONALE]. Intero. DEVE contenere un timestamp Unix che indica la data di inizio validità della delega;

- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica la data di fine validità della delega.

Tipologia di Delega	Attributo
Delegato generico	general_delegate
Esercente la responsabilità genitoriale	parental_authority_holder
Tutore del minore	minor_legal_guardian
Tutore dell'interdetto	incapacitated_person_guardian
Curatore	incapacitated_person_curator
Amministratore di sostegno	support_administrator
Procuratore generale	general_power_of_attorney_holder
Procuratore speciale	special_power_of_attorney_holder

Tabella 1 tipologia di delega

Di seguito, un esempio non normativo della risposta:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
      "delegation_info":"$DelegationDataResponseJWT"
}
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Livelli di Operatività della Delega

Di seguito sono descritti gli scopi della Delega Generale ed i Livelli di operatività FSE/EDS/PNT.

Le deleghe generali sono gestite con livelli di accesso indipendenti rispetto ai servizi relativi alle deleghe specifiche dell'ambito sanitario.

É, dunque, possibile creare una delega ai soli servizi della pubblica amministrazione, ai soli servizi in ambito sanitario o a entrambe

Scopi della Delega Generale

In fase di creazione delle deleghe, nel caso di delegato generico (general_delegate), il delegante PUÒ specificare il livello di operatività della delega tra le seguenti opzioni:

- Nessun accesso: il delegato non può accedere ai servizi online della pubblica amministrazione per conto del delegante;
- sola consultazione: il delegato può accedere ai servizi in modalità di sola lettura/consultazione delle informazioni del delegante;
- completo: il delegato può operare con i medesimi privilegi del delegante, incluse operazioni di modifica, inserimento e gestione.

Per le seguenti tipologie di delega, il livello di operatività DEVE essere completo:

- Esercente la responsabilità genitoriale (parental_authority_holder);
- Tutore del minore (minor_legal_guardian);
- Tutore dell'interdetto (incapacitated_person_guardian);
- Curatore (incapacitated_person_curator);
- Amministratore di sostegno (support_administrator);
- Procuratore generale (general_power_of_attorney_holder);
- Procuratore speciale (special_power_of_attorney_holder).

Livelli di Operatività in Ambito FSE/EDS/PNT

In conformità all'art. 11, comma 12 del "Decreto del Ministero della Salute del 7 settembre 2023" pubblicato in Gazzetta Ufficiale Serie Generale n. 249 del 24 ottobre 2023, per Fascicolo Sanitario Elettronico (FSE), Ecosistema Dati Sanitari (EDS), Piattaforma Nazionale di Telemedicina (PNT) è previsto un oggetto informativo separato, applicabile esclusivamente alle deleghe di tipo general_delegate.
Il delegante, in fase di creazione della delega, PUÒ specificare uno dei seguenti livelli di delega per l'accesso ai servizi in ambito FSE/EDS/PNT:

- Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato;

Oppure, in alternativa alla delega di tipo "O":

Per l'accesso ai servizi del FSE

- Delega di tipo “A”: Accesso completo al FSE dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati, gestione consensi e relative revoche);
  Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (anche insieme)
- Delega di tipo “B”: Consultazione dei dati e dei documenti relativi all’assistito presenti nel FSE;
- Delega di tipo “C”: Accesso alla gestione dei consensi e le relative revoche, oscuramenti e relative revoche del FSE, nonché l’ulteriore diritto di accesso alle informazioni relative alle operazioni di cui all'art. 21 del decreto del 7 settembre 2023, come previsto dall’art. 9, comma 1, del medesimo decreto;
- Delega di tipo “C-bis”: Accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica (art. 11, comma 2, Decreto del ministero Salute 7 settembre 2023)
- Delega di tipo “D”: Inserimento dei dati e documenti nel taccuino personale dell’assistito presente nel suo FSE.

Per l'accesso ai servizi EDS

- Delega di tipo “A-bis”: Accesso completo all’EDS dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);
  Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):
- Delega di tipo “B-bis”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nel EDS (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-ter”: Accesso alla gestione dei consensi e le relative revoche dell’EDS;

Per l'accesso ai servizi PNT

- Delega di tipo “A-ter”: Accesso completo alla PNT dell’assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi, gestione consensi e relative revoche);
  Oppure, nel caso il delegante intenda selezionare solamente le singole funzioni senza i massimi privilegi, è possibile la scelta tra (in alternativa tra loro):
- Delega di tipo “B-ter”: Accesso ai servizi e consultazione dei dati relativi all’assistito presenti nella PNT (esclusa gestione dei consensi e relative revoche);
- Delega di tipo “C-quater”: Accesso alla gestione dei consensi e le relative revoche della PNT;

Chiarimenti applicativi:
- con riferimento alla delega di tipo "A" l'accesso è completo in base alle previsioni di cui all'articolo 11, comma 12, lettera a), del Decreto del Ministero della Salute del 7 settembre 2023 e, pertanto, l'ambito di operatività della delega è, al pari dell'assistito, per la consultazione dei dati e dei documenti relativi all'assistito, inserimento di dati e documenti nel taccuino personale dell'assistito, nonché accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche e include la delega all'accesso ai servizi sanitari on-line resi disponibili dalle regioni e dalle province autonome in modalità telematica di cui al comma 2 del medesimo articolo 11.
- con riferimento alla delega di tipo “A-ter” o "B-ter", l'accesso consente altresì al delegato di supportare l’assistito delegante nell’accesso ai servizi di assistenza in telemedicina resi disponibili tramite la PNT. A titolo esemplificativo, il *caregiver* munito di delega "A-ter" o "B-ter" potrebbe autenticarsi in qualità di delegato, agevolando l’accesso dell’assistito al servizio di televisita.

Le deleghe di tipo B, C, C-bis, e D possono essere selezionate singolarmente o in combinazione tra loro, in base alla volontà del delegante e in conformità con l'art. 11, comma 12, lettere b), c) e d) del DM Salute del 7 settembre 2023 in alternativa alla delega di tipo A.
La delega di tipo B-bis e C-ter possono essere selezionate singolarmente, in base alla volontà del delegante, in alternativa alla delega di tipo A-bis.
La delega di tipo B-ter e C-quater possono essere selezionate singolarmente, in base alla volontà del delegante, in alternativa alla delega di tipo A-ter.
Le deleghe di tipo "A", A-bis e A-ter possono essere selezionate singolarmente oppure combinate tra loro e/o con le altre tipologie di delega selezionate in alternativa.
La delega di tipo 0, invece, è mutuamente esclusiva pertanto, la PGD NON DEVE consentire che questa venga combinata con altri livelli di delega.

Per le seguenti tipologie di delega, il livello di delega per l'ambito FSE/EDS/PNT è SEMPRE di tipo **A** (accesso completo):

- Esercente la responsabilità genitoriale (parental_authority_holder);
- Tutore del minore (minor_legal_guardian);
- Tutore dell'interdetto (incapacitated_person_guardian);
- Curatore (incapacitated_person_curator);
- Amministratore di sostegno (support_administrator);
- Procuratore generale (general_power_of_attorney_holder);
- Procuratore speciale (special_power_of_attorney_holder).

Durante la fase di onboarding il SP che fornisce servizi in ambito FSE/EDS/PNT DEVE aggiungere il seguente parametro nella richiesta di onboarding definita in sezione Endpoint di Onboarding:

- **health_delegation_type_required**: [OPZIONALE]. Booleano. Se true, il SP esprime la volontà di accedere ai dati di delega relativi all'ambito FSE/EDS/PNT. La PGD DEVE effettuare le opportune verifiche in merito all'autorizzazione del SP a fornire servizi in tale ambito. A tal fine la PGD DEVE effettuare almeno la verifica della presenza del SP all'interno di un apposito elenco interno (whitelist) dei SP abilitati ai servizi nell'ambito FSE/EDS/PNT. Le informazioni relative alla suddetta whitelist sono pubblicate sul Portale.

Integrazioni al delegation_info JWT

Alla struttura del JWT **delegation_info** definita nella sezione Get Delegation Data Endpoint si aggiungono i seguenti parametri:

- **delegation_scope**: [CONDIZIONALE]. Stringa. Se la delega è di tipo general_delegate, DEVE essere presente. Valori ammessi: "no_access" (nessun accesso ai servizi generali), "read_only" (solo consultazione) o "full_access" (completo) come definito in sezione Scopi della Delega Generale. Il valore "no_access" indica che il delegato non può operare sui servizi della pubblica amministrazione;
- **health_delegation_type**: [CONDIZIONALE]. Array di Stringhe. Se la delega è di tipo general_delegate e il SP gestisce servizi in ambito FSE/EDS/PNT, DEVE essere presente. I valori ammessi sono definiti nella sezione Livelli di Operatività in Ambito FSE/EDS/PNT. I valori "A", "A-bis" e "A-ter" POSSONO essere combinati tra loro o con altri valori ammessi e, nello specifico: I

valori “B”, “C”, “C-bis”, “D” POSSONO essere combinati tra loro ma NON DEVONO essere combinati con il valore “A”; il valore “C-ter” NON DEVE essere combinato con il valore “A-bis”; Il Valore “C-quater” NON DEVE essere combinato con il valore “A-ter”. Il valore “0” DEVE essere utilizzato singolarmente. Altre combinazioni NON DEVONO essere ammesse. Se il parametro è assente, si intende che il Service Provider non gestisce servizi in ambito FSE/EDS/PNT. Ai fini dell'invio dei dati di delega in ambito FSE/EDS/PNT, la PGD DEVE verificare che il SP richiedente sia presente in un apposito elenco interno (whitelist) dei SP abilitati alla ricezione di tali dati. In assenza di tale riscontro, la PGD NON DEVE includere i dati della delega FSE/EDS/PNT (parametro health_delegation_type nel JWT delegation_info) nella risposta trasmessa all'IdP.

Un esempio non normativo completo del payload del delegation_info JWT è dato di seguito.

```
{
  "iss": "https://pgd.example.it",
  "aud": "https://idp.example.it",
  "version": "1.0",
  "delegate": {
    "name": "Mario",
    "family_name": "Rossi",
    "birthdate": "1965-12-10",
    "fiscal_number": "RSSMRA65T10H027X"
  },
  "delegator": {
    "name": "Giuseppe",
    "family_name": "Verdi",
    "birthdate": "1975-05-20",
    "fiscal_number": "VRDGPP75E20F205A"
  },
  "delegation_type": "general_delegate",
  "delegation_scope": "full_access",
  "health_delegation_type": ["B", "C"],
  "delegation_created_at": 1734960000,
  "iat": 1734963600,
  "nbf": 1734963600,
  "exp": 1734963900
}
```

Integrazioni in SAML e OIDC

Alle informazioni di **delegationInfo** definite nella sezione Protocollo di scambio tra SP e IdP si aggiungono i seguenti attributi:

Per SAML:

```
<saml2:Attribute FriendlyName="Ambito Operatività Delega"
  Name="delegationInfo.delegationScope"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml2:AttributeValue
xsi:type="xs:string">full_access</saml2:AttributeValue>
```

```
</saml2:Attribute>

<saml2:Attribute FriendlyName="Tipo Delega Sanitaria"
  Name="delegationInfo.healthDelegationType"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml2:AttributeValue xsi:type="xs:string">A</saml2:AttributeValue>
</saml2:Attribute>
```

Per OIDC:

I parametri **delegation_scope** e **health_delegation_type** devono essere inclusi nel payload del JWT **delegation_info** trasmesso tramite il claim dedicato.

Nota: il parametro **delegation_scope** è sempre presente nel JWT **delegation_info** per le deleghe di tipo **general_delegate**, in quanto definisce il livello di operatività generale applicabile a tutti i servizi.
Il parametro **health_delegation_type** è presente nel JWT **delegation_info** solo se il delegante ha esplicitamente configurato la delega per l'ambito FSE/EDS/PNT durante la fase di creazione della delega.
Per i SP che non gestiscono servizi FSE/EDS/PNT, il parametro **health_delegation_type** sarà assente dal JWT, garantendo la minimizzazione dei dati trasmessi.

Distribuzione Chiave Pubblica PGD

Pubblicazione

La PGD DEVE pubblicare le proprie chiavi pubbliche utilizzate per la gestione dell'abilitazione e del ciclo di vita dei SP, e del protocollo di comunicazione con gli IdP in una apposita sezione del sito istituzionale della PGD.

Il formato di pubblicazione DEVE includere per ogni chiave:

- kid (Key ID in formato UUID v4);
- Algoritmo di firma;
- Chiave pubblica in formato JWK conforme a [RFC7517];
- Fingerprint SHA-256 della chiave;
- Periodo di validità.

Gli IdP e gli SP DEVONO configurare la chiave nei propri sistemi per consentire le verifiche previste durante i protocolli di scambio dati.
Per scopi di interoperabilità, PGD PUÒ rendere disponibili le proprie chiavi pubbliche anche tramite l'endpoint well-known "/.well-known/jwks.json", che DEVE restituire le chiavi pubbliche in formato JWKS.

I SP e gli IdP DEVONO verificare la corrispondenza tra le chiavi pubbliche esposte tramite l'endpoint well-known e quelle acquisite tramite i canali out-of-band. La PGD deve garantire l'allineamento tra le chiavi esposte su entrambe i canali. I SP e gli Id in caso di disallineamento la PGD DEVE considerare non valida la chiave e interrompere l'operazione con errore.

Rotazione Chiavi e Notifica agli SP e agli IdP

In caso di rotazione delle chiavi di firma, la PGD DEVE:

1. Pubblicare la nuova chiave in una apposita sezione del portale istituzionale di PGD mantenendo la chiave precedente;
2. Inviare notifica agli SP tramite l'indirizzo email registrato e agli IdP tramite i contatti pubblicati nei metadata ufficiali;
3. Firmare Registro JWT e Trust Mark con entrambe le chiavi (nuova e precedente) per un periodo di overlap;
4. Dopo il periodo di overlap, rimuovere la chiave precedente.

Il periodo di overlap DEVE essere di almeno 60 giorni.

Quando la PGD pubblica una nuova chiave, DEVE inviare una notifica all'indirizzo di contatto degli IdP e a quello registrato da ciascun SP durante l'onboarding.
La notifica DEVE contenere almeno le seguenti informazioni:

- kid della nuova chiave;
- Fingerprint SHA-256;
- URL di download;
- Periodo di overlap (almeno 60 giorni);
- Data scadenza chiave precedente.

Gli SP e IdP DEVONO verificare il fingerprint con i riferimenti pubblicati sui canali istituzionali e di conseguenza aggiornare la propria configurazione aggiungendo la nuova chiave entro il periodo di overlap.

Gestione abilitazione dei servizi

Una volta ricevuti tutti gli attributi trasmessi dalla Piattaforma Gestione Deleghe, ricade sotto la responsabilità esclusiva del Service Provider (SP) la determinazione delle logiche di autorizzazione all'accesso ai servizi erogati, in particolare:

- Individuare eventuali servizi che non siano compatibili con l'accesso tramite delega, valutato il contesto, le finalità, le tipologie dei dati trattati e gli eventuali impatti sulla sfera giuridica del delegante e/o di terzi e, di conseguenza, non consentirne l'accesso, anche non accettando gli attributi trasmessi dalla Piattaforma;

- Eventualmente limitare funzionalmente il servizio in rete erogato (es. consentire la sola consultazione inibendo le funzionalità dispositive) sulla base degli attributi ricevuti dalla Piattaforma (tipologia di delega, perimetro di utilizzo, validità);
- Tracciare le attività di sistema mediante la definizione di una policy formale che garantisca la conservazione sicura dei log, incluse modalità di accesso per la loro consultazione, per almeno 24 mesi, documentando le procedure tecniche a tutela dell'integrità e disponibilità del dato, inclusa la registrazione obbligatoria della motivazione sottesa a qualsiasi accesso alle da parte degli operatori.

Notifiche

Il sistema DEVE implementare un meccanismo di notifica che, nei casi previsti dalla norma, informi gli utenti dell'accesso ai dati della PGD, dando evidenza del nome del SP e dell'IdP utilizzato dal delegato.
La notifica DEVE riportare i riferimenti all'informativa sul trattamento dei dati personali e la descrizione delle modalità per eventualmente revocare una delega conferita.

Logging

Il sistema PDG DEVE implementare un meccanismo di logging che registri i comportamenti anomali, gli errori e le operazioni significative in maniera tale da poter garantire la tracciabilità e la diagnostica dei vari dettagli salienti del flusso di utilizzo della delega in accordo con le misure previste da [Allegato 4].

Specifiche IdP

Ai sensi dell'articolo 13, comma 2, del decreto 23 febbraio 2026, l'integrazione dell'IdP con la PGD non modifica la disciplina relativa alla titolarità dei trattamenti. Ciascun IdP opera quale autonomo titolare per i trattamenti effettuati nell'ambito delle attività di propria competenza connesse all'autenticazione dell'utente e alla gestione dell'accesso ai servizi in regime di delega. L'IdP DEVE pubblicare sul proprio portale istituzionale, rendendola facilmente accessibile all'utente, un'informativa sul trattamento dei dati personali redatta anche ai sensi dell'articolo 14 del Regolamento (UE) 2016/679 (GDPR). Tale informativa DEVE specificare le finalità e le modalità del trattamento dei dati riferiti al soggetto Delegato e Delegante nell'ambito della gestione degli accessi per conto terzi.
Nelle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi, conservate come da normativa vigente, L'IdP DEVE garantire la conservazione anche delle informazioni necessarie alle attività svolte in regime di delega.
Tali evidenze, riportando gli identificativi univoci della transazione, le date di emissione (Timestamp) e i dati relativi alla delega (is_delegate e relativi attributi), costituiscono prova tecnica opponibile per l'accertamento dell'identità del soggetto agente (Delegato) e del titolo autorizzativo (Delega).

Meccanismi di informazione tra soggetti

Al fine di garantire una corretta gestione degli incidenti di sicurezza e delle violazioni di dati personali connesse all'utilizzo della Piattaforma Gestione Deleghe (PGD), DEVONO essere previsti meccanismi di informazione tempestiva e reciproca tra il Gestore della Piattaforma, gli Identity Provider (IdP) e i Service Provider (SP).
I presenti meccanismi si applicano a:

- violazioni di dati personali relative ai trattamenti effettuati tramite la PGD;
- incidenti di sicurezza che possano incidere su disponibilità, integrità, riservatezza o autenticità dei dati e dei servizi coinvolti nei flussi PGD-IdP-SP;

fermo restando che gli obblighi di notifica verso Autorità e interessati rimangono in capo ai rispettivi titolari del trattamento.
Il Gestore, ciascun IdP e ciascun SP DEVONO:

- designare almeno un punto di contatto tecnico e, ove previsto, uno organizzativo/privacy;
- mettere a disposizione un canale di comunicazione che garantisca autenticità del mittente e integrità dei messaggi (es. PEC o canale equivalente).

Tali informazioni DEVONO essere mantenute aggiornate e rese disponibili agli altri soggetti coinvolti.

Algoritmi Supportati

Per la specifica degli algoritmi di firma supportati dal protocollo di rimanda alle specifiche disponibili nella Sezione Algoritmi Crittografici e Linee guida funzioni crittografiche di ACN.

Gestione degli aggiornamenti della Specifica

Queste specifiche tecniche possono essere aggiornate per motivi di sicurezza, evoluzione tecnologica o conformità a standard nazionali ed europei, nel rispetto dei principi e requisiti definiti dalla normativa di riferimento. Gli aggiornamenti DEVONO essere pubblicati sul Portale della Piattaforma di Gestione Deleghe.

Acronimi

ACRONIMO	DEFINIZIONE
ACN	Agenzia per la Cybersicurezza Nazionale
CIE	Carta di Identità Elettronica
CSRF	Cross-site Request Forgery

DPoP	Demonstrating Proof-of-Possession
IdP	Gestore delle identità digitali (Identity Provider). Sinonimo di OpenID Provider (OP), secondo il protocollo OIDC
JWKS	JSON Web Key Set
JWT	JSON Web Token
MiTM	Man in The Middle
OIDC	OpenID Connect
PAR	Pushed Authorization Requests secondo quanto definito da OAuth 2.0 Pushed Authorization Requests (PAR) [RFC9126]
PGD	Piattaforma Gestione Deleghe
PKCE	Proof Key for Code Exchange
RP	Relying Party, sinonimo di Service Provider (Vedi anche acronimo SP)
SAML	Security Assertion Markup Language
SP	Fornitore di servizi digitali (Service Provider)
TM	Trust Mark
OTP	One-Time Password
FSE	Fascicolo Sanitario Elettronico
PNT	Piattaforma Nazionale Telemedicina
EDS	Ecosistema Dati Sanitari

IL SOTTOSEGRETARIO DI STATO ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI
CON DELEGA ALL'INNOVAZIONE TECNOLOGICA

DI CONCERTO CON
IL MINISTRO DELLA GIUSTIZIA

Disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe

Il Presidente del Consiglio dei ministri

VISTA la legge 24 agosto 1988, n. 400, recante "Disciplina dell'attività di Governo e ordinamento della
Presidenza del Consiglio dei ministri"

VISTO il decreto legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale", e, in particolare, l'articolo 64-*ter,* con cui è stata istituita la Piattaforma di gestione deleghe;

VISTO il decreto-legge 2 marzo 2024, n. 19 convertito, con modificazioni, dalla legge 29 aprile 2024, n. 56 ed in particolare, l'articolo 20, comma 1, lettera d) che ha sostituito l'articolo 64-ter del decreto legislativo 7 marzo 2005, n. 82;

VISTA la legge 5 febbraio 1992, n. 194 e successive modificazioni, recante "legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate";

VISTO il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante il "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

VISTO il decreto-legge 6 maggio 2021, n. 59, recante "Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti", convertito, con modificazioni, dalla legge 1° luglio 2021, n. 101;

VISTO il decreto-legge 31 maggio 2021, n. 77, recante "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;

VISTA la legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";

VISTO il decreto del Ministro della giustizia 21 febbraio 2011, n. 44, recante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24" nonché le specifiche tecniche adottate ai sensi dell'articolo 34, comma 1, del citato decreto ministeriale 21

febbraio 2011, n. 44 e contenute nel Provvedimento DGSIA del 16 aprile 2014 e s.m.i.;

VISTO il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale 27 giugno 2024, n. 21007, recante "Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221";

VISTO il decreto del Presidente del Consiglio dei ministri 1° ottobre 2012, concernente l'ordinamento delle strutture generali della Presidenza del Consiglio dei ministri;

VISTO il decreto del Presidente della Repubblica 31 ottobre 2022, con il quale l'On. Giorgia Meloni è stata nominata Presidente del Consiglio dei ministri;

VISTO il decreto del Presidente della Repubblica 31 ottobre 2022, con il quale il Sen. Alessio Butti è stato nominato Sottosegretario di Stato alla Presidenza del Consiglio dei ministri;

VISTO il decreto del Presidente del Consiglio dei ministri 25 novembre 2022 concernente la delega di funzioni in materia di innovazione tecnologica e transizione digitale al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, Sen. Alessio Butti;

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;

VISTO il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - GDPR);

CONSIDERATA la necessità di novellare le previsioni di cui al decreto 30 marzo 2022 del Ministro per l'innovazione tecnologica e la transizione digitale di concerto con il Ministro dell'Interno recante "Disciplina delle modalità di funzionamento del Sistema di Gestione Deleghe ("SDG") emanato ai sensi della previgente normativa sulle quali l'Autorità Garante per la protezione dei dati personali si era espresso con i provvedimenti n. 74 del 24 febbraio 2022, doc. web. n. 9752853 e n. 330 del 6 ottobre 2022, doc. web. n. 9823221.

CONSIDERATA la necessità di dare attuazione a quanto disposto al novellato comma 6 del citato articolo 64-*ter* del decreto legislativo 7 marzo 2005, n. 82, che rinvia a un successivo decreto del Presidente del Consiglio dei ministri ovvero dell'Autorità politica delegata in materia di innovazione tecnologica, da adottarsi di concerto con il Ministro della giustizia, sentiti il Garante per la protezione dei dati personali e l'Agenzia per la cybersicurezza nazionale, la disciplina delle caratteristiche tecniche, dell'architettura generale, dei requisiti di sicurezza, delle modalità di funzionamento della

piattaforma di cui al comma 5, nonché delle tipologie di dati oggetto di trattamento e, in generale, delle modalità e delle procedure per assicurare il rispetto dell'articolo 5 del regolamento (UE) 2016/679;

SENTITA l'Agenzia per la cybersicurezza nazionale, che si è espressa con nota del Direttore Generale del 29 maggio 2025;

SENTITO il Garante per la protezione dei dati personali, che ha reso il parere di competenza con provvedimento n. 66 del 12 febbraio 2026;

ACQUISITO il concerto del Ministro della giustizia in data 19 febbraio 2026.

DECRETA

Art. 1
(*Definizioni)*

1. Ai fini del presente decreto si intendono per:
   a. "CAD": il decreto legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale";
   b. "ANPR": l'Anagrafe Nazionale della Popolazione Residente di cui all'articolo 62 del CAD;
   c. "Gestore dell'identità digitale": il soggetto che rende disponibile e gestisce l'identità digitale SPID o CIEid ai sensi di legge;
   d. "Gestore della Piattaforma": l'Istituto Poligrafico e Zecca dello Stato S.p.A. (IPZS);
   e. "PDND": la Piattaforma Digitale Nazionale Dati di cui all'articolo 50-*ter* del CAD;
   f. "Piattaforma": la piattaforma di gestione delle deleghe di cui all'articolo 64-*ter* del CAD;
   g. "Portale": l'interfaccia web della Piattaforma di gestione deleghe, accessibile all'indirizzo: https://deleghedigitali.gov.it;
   h. "Pubbliche amministrazioni": i soggetti di cui all'articolo 2, comma 2, del CAD.
   i. "delega": la delega di cui all'articolo 64-ter del CAD ai Servizi in rete erogati dalle pubbliche amministrazioni, inclusa l'abilitazione all'accesso del soggetto munito di procura generale o speciale, dell'esercente la responsabilità genitoriale, del tutore del minore, del tutore dell'interdetto, del curatore dell'inabilitato e dell'amministratore di sostegno; sono escluse le deleghe professionali e i mandati conferiti a soggetti che operano quali professionisti o intermediari abilitati, ivi compresi gli incarichi conferiti ai sensi di contratti d'opera intellettuale o di servizi oppure a istituti di patronato e assistenza sociale.
   l. "procura speciale": la procura speciale rilasciata in forma di atto pubblico o scrittura privata autenticata relativa all'accesso ai Servizi in rete di cui al presente decreto.

m. "Servizi in rete": i servizi digitali destinati esclusivamente ai cittadini; sono esclusi i servizi e le funzionalità destinati a professionisti, lavoratori, dipendenti, professionisti e collaboratori a vario titolo, per lo svolgimento di attività professionali, per compito di interesse pubblico o in attuazione di un obbligo di legge.

Art. 2
(*Oggetto e ambito di applicazione*)

1. Il presente decreto disciplina le modalità di funzionamento della Piattaforma, definendone le caratteristiche tecniche, l'architettura generale, i requisiti di sicurezza, le tipologie di dati oggetto di trattamento, le categorie di interessati e, in generale, le modalità e le procedure per assicurare il rispetto dell'articolo 5 del regolamento (UE) 2016/679.

Art. 3
(*Presentazione della delega tramite il Portale*)

1. Il cittadino iscritto nell'ANPR può delegare l'accesso ai Servizi in rete erogati dalle pubbliche amministrazioni che richiedono l'identificazione informatica in favore di non più di due soggetti iscritti nell'ANPR, utilizzando le specifiche funzionalità rese disponibili dal Portale.
2. Le funzionalità di cui al comma 1 consentono:
    a. al delegante, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo, di presentare la delega in favore di un soggetto, che la accetta entro trenta giorni, previo accesso al Portale tramite le medesime modalità. In tale caso, la delega è registrata nella Piattaforma al momento dell'accettazione da parte del delegato;
    b. al delegato, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo, di presentare la delega ricevuta dal delegante tramite documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata o avanzata realizzata ai sensi dell'articolo 16 del decreto del ministero dell'Interno 8 settembre 2022 dal delegante o comunque dal notaio o da altro pubblico ufficiale autorizzato ad autenticare la firma ai sensi dell'articolo 25 del CAD. In tale caso, la delega è registrata nella Piattaforma al momento della verifica dei documenti e della validità delle sottoscrizioni;
    c. al genitore esercente la responsabilità genitoriale e al tutore del minore, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo, di presentare la delega al fine di accedere ai servizi per conto del minore a seguito della verifica delle relative informazioni rese disponibili dall'ANPR e all'esito positivo della verifica delle informazioni rese

disponibili dal Ministero della giustizia in riferimento all'assenza di provvedimenti che prevedono la perdita della responsabilità genitoriale, la decadenza dalla stessa o la sospensione dal suo esercizio. In tale caso, la delega è registrata nella Piattaforma all'esito positivo della verifica svolta dalla Piattaforma mediante i servizi della PDND. Fino alla messa a disposizione delle informazioni da parte del Ministero della giustizia ai sensi dell'articolo 7, il genitore esercente la responsabilità genitoriale dichiara ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 la propria qualità;

d. al tutore, al curatore dell'inabilitato e all'amministratore di sostegno, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD, con livello di sicurezza almeno significativo, di presentare la delega al fine di accedere ai servizi per conto dell'interdetto, dell'inabilitato o del beneficiario. In tale caso, la delega è registrata nella Piattaforma all'esito positivo della verifica delle informazioni rese disponibili dal Ministero della giustizia, effettuata dalla Piattaforma mediante i servizi della PDND;
e. al genitore esercente la responsabilità genitoriale, al tutore, al curatore dell'inabilitato e all'amministratore di sostegno, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo, di presentare la delega ad operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno in favore di un altro soggetto, che la accetta, previo accesso al Portale tramite le medesime modalità. In tale caso, la delega è registrata nella Piattaforma al momento dell'accettazione da parte del delegato, previo esito positivo della verifica svolta dalla Piattaforma mediante i servizi della PDND in ordine alla qualifica rivestita dal soggetto delegante.

3. La presentazione della delega di cui al comma 2 può avvenire anche tramite il punto di accesso telematico per i dispositivi mobili previsto dall'articolo 64-*bis* del CAD, mediante interoperabilità con i sistemi della Piattaforma ai sensi della normativa vigente.
4. Fatto salvo quanto previsto dal comma 2, lettera e), il delegato non può subdelegare l'accesso ai Servizi in rete erogati dalle pubbliche amministrazioni che richiedono l'identificazione informatica del delegante.

Art. 4

(Presentazione della delega con l'assistenza remota del Gestore della Piattaforma)

1. Fermo restando quanto previsto dall'articolo 5, al fine di agevolare la presentazione della delega di cui all'articolo 64-*ter* del CAD da parte dei soggetti più fragili, il cittadino iscritto nell'ANPR di età pari o superiore ai 65 (sessantacinque) anni o in possesso di certificazione

rilasciata ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n. 104, può richiedere di presentare la delega con l'assistenza remota del Gestore della Piattaforma, tramite un apposito servizio reso disponibile nel Portale.

2. Nel caso di cui al comma 1, il delegato iscritto nell'ANPR, previo accesso allo specifico servizio del Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo e inserimento del numero identificativo della carta di identità del delegante, richiede l'assistenza del Gestore della Piattaforma per effettuare la registrazione della delega ricevuta dal soggetto delegante iscritto nell'ANPR in conformità a quanto previsto dall'Allegato 1 e selezionando una tra le date e orario disponibili indicate dal Gestore medesimo nell'apposita area dedicata del Portale. In tale caso, l'erogazione del servizio è confermata all'esito positivo della verifica della validità del numero identificativo della carta di identità del delegante svolta dalla Piattaforma mediante i servizi della PDND.
3. L'erogazione del servizio nella data e orario selezionati dal delegato ai sensi del comma 2 richiede la necessaria copresenza del delegato e del delegante e la capacità di quest'ultimo di interagire ed esprimere, in piena consapevolezza, la sua volontà di delega nonché la disponibilità di un dispositivo con connessione Internet, munito di videocamera, microfono ed eventuali cuffie o altoparlanti. In mancanza di tali supporti o qualora, in fase di accesso al servizio in video, il delegante e il delegato non diano l'assenso alla registrazione, il servizio non potrà essere erogato nella modalità richiesta.
4. L'operatore addetto del Gestore della Piattaforma, opportunamente selezionato e formato sulle responsabilità inerenti al servizio di cui al presente articolo, anche qualora appartenente a soggetti terzi di cui il Gestore si avvalga per l'erogazione del servizio, registra la volontà della delega insieme alla copia informatica per immagine del documento d'identità del delegante e del delegato che dovranno essere esibiti anche in originale a video con le modalità e le garanzie di cui all'Allegato 1. Il Gestore della Piattaforma effettua controlli, anche a campione, sul corretto svolgimento delle operazioni di cui al presente comma in relazione a una percentuale non inferiore al 5 percento delle deleghe così registrate nella Piattaforma.
5. A seguito della conclusione delle operazioni e all'esito della positiva verifica ~~dei documenti~~ dei requisiti di cui al comma 1, il Gestore della Piattaforma registra la delega nella Piattaforma.
6. Le disposizioni di cui al presente articolo non si applicano alle deleghe presentate da esercenti la responsabilità genitoriale, tutori, curatori e amministratori di sostegno ai sensi dell'articolo 3, comma 2, lettere c) e d).

Art. 5

(*Presentazione della delega tramite il comune di residenza*)

IL SOTTOSEGRETARIO DI STATO ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI
CON DELEGA ALL'INNOVAZIONE TECNOLOGICA

DI CONCERTO CON
IL MINISTRO DELLA GIUSTIZIA

1. Il cittadino iscritto nell'ANPR può delegare l'accesso ai Servizi in rete erogati dalle pubbliche amministrazioni che richiedono l'identificazione informatica a non più di due soggetti iscritti nell'ANPR, recandosi presso il comune di residenza e sottoscrivendo la relativa richiesta con firma autografa apposta in presenza del dipendente addetto al procedimento. Il delegante esibisce, inoltre, il proprio documento d'identità. La medesima richiesta può essere sottoscritta dal solo delegato che, presso il Comune di residenza del delegante, esibisca copia della procura generale o speciale. In tal caso il procuratore, ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, dichiara che la propria qualità è tuttora sussistente e che non sono intervenute modifiche o revoche;
2. Nel caso di cittadini iscritti nell'ANPR allettati per lunga durata, ricoverati o impossibilitati per motivi sanitari a recarsi presso il comune di residenza, la delega può essere presentata direttamente dal delegato anche mediante acquisizione, da parte del dipendente addetto al procedimento del comune di residenza del delegante, della delega sottoscritta dal delegante unitamente alla copia del proprio documento d'identità e di una attestazione sanitaria secondo il formato standard di cui all'Allegato 2 redatta da un medico del servizio sanitario nazionale attestante l'impossibilità del delegante di recarsi presso lo sportello o di certificazione rilasciata al delegante ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n. 104. Il delegato, inoltre, esibisce il proprio documento d'identità.
3. Il comune di residenza rigetta le richieste pervenute secondo altre forme e, in tale caso, invita il cittadino a presentare la delega utilizzando le specifiche funzionalità rese disponibili dal Portale secondo quanto previsto dagli articoli 3 e 4.
4. Mediante le funzionalità rese disponibili dal Gestore della Piattaforma ai comuni anche utilizzando le infrastrutture di cui al decreto del Ministero dell'Interno del 23 dicembre 2015 recante "Modalità tecniche di emissione della Carta d'identità elettronica", il dipendente addetto al procedimento del comune di residenza, opportunamente formato sulle responsabilità inerenti al servizio di cui al presente articolo, inserisce nel Portale la delega presentata ai sensi dei commi 1 e 2, contestualmente alla ricezione della richiesta o comunque entro tre giorni dalla ricezione della stessa, allegando copia su supporto informatico prodotta ai sensi dell'articolo 22, comma 1, del CAD della documentazione presentata dal delegante o dal delegato secondo il presente articolo. Ai sensi dell'articolo 22, comma 4, e dell'articolo 23-*ter*, comma 3, del CAD, l'obbligo di conservazione dell'originale dei documenti così allegati è soddisfatto e viene meno il conseguente obbligo di conservazione da parte del comune dei documenti originali analogici.
5. Il delegato, previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo, accetta la delega inserita nel Portale ai sensi del comma 4. In tale caso, la delega è registrata nel Portale al momento

dell'accettazione da parte del delegato e di tale registrazione è data notizia al comune di residenza competente, che informa il delegante dell'esito della pratica.

6. La registrazione della delega di cui all'articolo 3, comma 2, lettere c) e d) può essere effettuata dal delegato recandosi presso il comune di residenza del delegante e sottoscrivendo la relativa richiesta con firma autografa apposta in presenza del dipendente addetto al procedimento. Il delegato esibisce, inoltre, il proprio documento d'identità.
7. I moduli tramite i quali è possibile richiedere la registrazione della delega presso il comune di residenza a norma del presente articolo sono conformi all'Allegato 3.

Art. 6

(*Verifica dell'iscrizione dei cittadini nell'ANPR da parte del Gestore della Piattaforma*)

1. Nei casi di presentazione della delega secondo le modalità di cui all'articolo 3, la verifica dell'iscrizione dei cittadini deleganti e delegati nell'ANPR da parte del Gestore della Piattaforma, tramite il relativo servizio della PDND, è effettuata:
    a. nel caso di cui al comma 1, lettera a), del medesimo articolo, all'atto della presentazione della delega da parte del delegante e al momento della sua accettazione da parte del delegato;
    b. nei casi di cui al comma 1, lettere b), c), d) ed e) del medesimo articolo, all'atto della presentazione della delega da parte del delegato.
2. Nei casi di presentazione della delega secondo le modalità di cui all'articolo 4, la verifica dell'iscrizione dei cittadini deleganti e delegati nell'ANPR da parte del Gestore della Piattaforma, tramite il relativo servizio della PDND, è effettuata all'atto della richiesta dell'assistenza del Gestore della Piattaforma di cui all'articolo 4, comma 2.
3. Nei casi di presentazione della delega secondo le modalità di cui all'articolo 5, la verifica dell'iscrizione dei cittadini deleganti e delegati nell'ANPR da parte del Gestore della Piattaforma, tramite il relativo servizio della PDND, è effettuata dal Gestore della Piattaforma al momento dell'inserimento della delega ai sensi dell'articolo 5, comma 4. Il comune di residenza verifica, in ogni caso, l'iscrizione del delegante e del delegato nell'ANPR contestualmente alla ricezione della richiesta e, se il delegato o il delegante non risultano iscritti, previa verifica della correttezza dei dati nell'ANPR, non procede all'inserimento di cui all'articolo 5, comma 4.
4. Nel caso in cui l'esito delle verifiche di cui ai commi 1, 2 e 3 effettuate dal Gestore della Piattaforma sia negativo, ne viene data comunicazione al cittadino, che è invitato a recarsi presso il proprio comune di residenza per le relative verifiche e la Piattaforma non consente la registrazione della delega.

5. La Piattaforma si avvale dei dati dell'ANPR, tramite il relativo servizio della PDND, al fine di ricevere giornalmente i dati afferenti ai soggetti deceduti e procedere al blocco tempestivo delle deleghe in corso di validità registrate a nome del soggetto deceduto in qualità di delegato o delegante. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per tali soggetti.
6. La Piattaforma si avvale dei dati dell'ANPR, tramite il relativo servizio della PDND, anche al fine di assicurare l'allineamento delle informazioni anagrafiche ai sensi dell'articolo 62, comma 5, del CAD quali, in particolare, quelle relative all'iscrizione del cittadino delegante e delegato nell'ANPR, all'identificativo univoco del cittadino (ID ANPR), al numero e data di scadenza della carta di identità e al domicilio digitale del cittadino ove presente.
7. La Piattaforma si avvale altresì dei dati dell'ANPR, tramite il relativo servizio della PDND, per le verifiche necessarie ai sensi dell'articolo 3, comma 2, lettera c), e riceve giornalmente i dati afferenti all'eventuale perdita, decadenza o sospensione della responsabilità genitoriale o all'avvenuta emancipazione del minore. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per conto di tali soggetti.

Art. 7
(Messa a disposizione *delle informazioni da parte del Ministero della giustizia e accesso del Gestore della Piattaforma*)

1. Ai fini della verifica della qualità di tutore, curatore o amministratore di sostegno e dell'assenza di provvedimenti che prevedono la perdita, la sospensione o la decadenza dalla responsabilità genitoriale del soggetto che presenta la delega nei casi di cui all'articolo 3, comma 2, lettere c), d) ed e), il Ministero della giustizia organizza e rende disponibili mediante i servizi della PDND le informazioni relative ai soggetti sottoposti a tutela, curatela e amministrazione di sostegno e ai rispettivi tutori, curatori e amministratori di sostegno e le relative sostituzioni, revoche e cessazioni, nonché le informazioni relative a provvedimenti che prevedono la perdita, la sospensione o la decadenza dalla responsabilità genitoriale e relative modifiche o revoche, unitamente ai dati identificativi e al codice fiscale dei soggetti interessati.
2. Le modalità di organizzazione delle informazioni di cui al comma 1 e quelle in cui le medesime informazioni sono rese disponibili sono definite dalle specifiche tecniche adottate dal capo del Dipartimento per l'innovazione tecnologica della giustizia del Ministero della giustizia.
3. Entro tre mesi dall'adozione delle specifiche tecniche di cui al comma 2, il Ministero della giustizia rende disponibili mediante i servizi della PDND le informazioni di cui al comma 1 risultanti da provvedimenti giudiziari adottati prima dell'entrata in vigore del presente decreto.
4. Contestualmente alla richiesta di registrazione della delega di cui all'articolo 3, comma 2, lettere c), d) ed e), il Gestore della Piattaforma fruisce, mediante i servizi della PDND, delle

informazioni rese disponibili dal Ministero della giustizia al fine di effettuare le verifiche previste dal comma 1. Successivamente alla registrazione della delega, il Gestore fruisce delle medesime informazioni al fine di ricevere tempestivamente i dati relativi alle cessazioni della qualifica di tutore, di curatore o di amministratore di sostegno o a provvedimenti che prevedono la perdita, la sospensione o la decadenza dalla responsabilità genitoriale e procedere all'immediata revoca della delega stessa. In caso di revoca della delega, i dati sono conservati per il tempo strettamente necessario all'esecuzione delle relative operazioni.

Art. 8
(*Registrazione della delega nella Piattaforma*)

1. La registrazione della delega nella Piattaforma avviene secondo le specifiche tecniche di cui all'articolo 11 e la conseguente registrazione da parte del Gestore della Piattaforma dei dati relativi all'avvenuta emissione e di quelli necessari al suo utilizzo e verifica ai sensi dell'articolo 9.
2. Per ciascun delegato possono essere registrate fino ad un massimo di cinque deleghe. Questa limitazione non si applica ai casi di deleghe presentate da esercenti la responsabilità genitoriale, tutori, curatori e amministratori di sostegno ai sensi dell'articolo 3, comma 2, lettere c) e d) nonché dai procuratori generali e speciali. All'atto di richiesta di registrazione della delega, il soggetto delegato dichiara, ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di agire a titolo personale e non nell'esercizio di attività professionale o d'impresa, e che la delega conferita non costituisce mandato professionale né è connessa a compenso o fatturazione.
3. Al fine di consentire ai cittadini di avere evidenza dell'uso della delega registrata e di tutelarli dall'uso illecito da parte di terzi, il Gestore della Piattaforma conserva le registrazioni delle richieste di utilizzo della delega da parte del delegato secondo quanto previsto dall'articolo 13 nonché le evidenze in merito alla gestione della delega da parte del delegante e del delegato.
4. I dati contenuti nel registro, compresi quelli personali, possono essere estratti dal registro esclusivamente su richiesta dell'autorità giudiziaria e delle autorità vigilanti, tramite personale espressamente incaricato ed appositamente dotato di credenziali di accesso personali. L'accesso a tali informazioni è registrato in appositi log.
5. I dati contenuti nel registro sono sempre consultabili su richiesta del delegante o del delegato anche previo accesso al Portale tramite l'identità digitale di cui all'articolo 64, comma 2-*quater*, del CAD con livello di sicurezza almeno significativo ovvero recandosi presso il Comune di residenza; l'accesso da parte del delegato può concernere esclusivamente informazioni riferite alle deleghe dallo stesso ricevute, con esclusione, quindi, di informazioni riferite alle deleghe che il medesimo delegante ha eventualmente conferito ad altro soggetto.

6. Della registrazione della delega nonché di ogni richiesta di utilizzo della stessa da parte del delegato viene data comunicazione al delegante tramite il proprio domicilio digitale, ove disponibile, ovvero all'eventuale recapito di contatto indicato dal delegante al momento della presentazione della delega; il presente comma non si applica ai casi di cui all'articolo 3, comma 2, lettere c), d) ed e).

Art. 9

(*Utilizzo della delega da parte del delegato*)

1. In occasione dell'accesso da parte del cittadino ai Servizi in rete erogati dalle pubbliche amministrazioni che richiedono l'identificazione informatica, il Gestore dell'identità digitale abilita la possibilità per il cittadino di scegliere se operare per conto di un soggetto delegante.
2. Nel caso in cui il cittadino scelga di operare per conto di un soggetto delegante ai sensi del comma 1, il Gestore dell'identità digitale interroga la Piattaforma per verificare la sussistenza, in capo al cittadino medesimo, di una delega valida, registrata nella Piattaforma ai sensi del presente decreto.
3. Nel caso in cui la verifica di cui al comma 2 dia esito positivo, l'accesso del soggetto delegato per conto del soggetto delegante al servizio in rete erogato dalla pubblica amministrazione avviene secondo le specifiche tecniche di cui all'articolo 11.
4. Il Gestore della Piattaforma rende disponibili al Sistema di portafoglio digitale italiano - Sistema IT-Wallet di cui all'articolo 64-quater del CAD, in qualità di Titolare di Fonte Autentica e secondo le linee guida approvate ai sensi del comma 3 del medesimo articolo 64-quater del CAD, i dati relativi alle deleghe registrate nella Piattaforma, al fine di consentirne l'utilizzo come Attestato Elettronico del portafoglio digitale del soggetto delegato per l'accesso ai servizi in rete e per l'attestazione dei poteri esercitabili per conto del soggetto delegante. I dati per la generazione e per la gestione del ciclo di vita dell'Attestato Elettronico relativo alle deleghe registrate è assicurato dal Gestore della Piattaforma, su richiesta dell'interessato, conformemente al piano di rilascio di cui all'articolo 14;
5. Ciascuna pubblica amministrazione classifica e mantiene aggiornato l'elenco dei propri Servizi in rete ai fini dell'accesso mediante delega, valutati i presupposti normativi, il contesto, le finalità e le tipologie di dati trattati dai servizi, secondo almeno le seguenti categorie: servizi delegabili a tutti, mediante delega conferibile ai sensi del presente decreto; servizi delegabili nell'ambito delle deleghe di cui all'articolo 3, comma 2, lettera c) (esercente la responsabilità genitoriale e tutore del minore); servizi delegabili nell'ambito delle deleghe di cui all'articolo 3, comma 2, lettera d) (tutore dell'interdetto, curatore dell'inabilitato e amministratore di sostegno) ovvero al procuratore generale o speciale; servizi non delegabili tramite i servizi della Piattaforma, in quanto soggetti a disciplina speciale ovvero a modalità di rappresentanza o di abilitazione diverse. Resta ferma la responsabilità delle pubbliche

amministrazioni in ordine alla verifica di compatibilità dei Servizi in rete con l'accesso in delega e alla determinazione delle conseguenti logiche di autorizzazione, inclusa l'eventuale limitazione delle funzionalità fruibili in delega, coerentemente con le informazioni messe a disposizione dai servizi della Piattaforma previste nell'Allegato 5. In caso di servizi classificati quali delegabili a tutti, mediante delega conferibile ai sensi del presente decreto, che comportano il trattamento dei dati personali di cui agli articoli 9 e 10 del regolamento (UE) 2016/679, le pubbliche amministrazioni effettuano o aggiornano la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del medesimo regolamento (UE) 2016/679.

6. Per i Servizi in rete relativi al Fascicolo sanitario elettronico, all'Ecosistema dati sanitari e alla Piattaforma nazionale di telemedicina, l'integrazione con i servizi della Piattaforma è realizzata, con riferimento alle fattispecie di cui all'articolo 3, comma 2, lettere c) (esercente la responsabilità genitoriale e tutore del minore) e d) (tutore dell'interdetto, curatore dell'inabilitato e amministratore di sostegno), nonché per i soggetti muniti di procura generale o speciale, per i quali è consentito al delegato l'accesso completo ai predetti servizi e funzionalità. Con riferimento, inoltre, alle fattispecie di cui all'articolo 3, comma 2, lettere a) e b), articolo 4, comma 1 e articolo 5, comma 1, primo periodo (relativi al delegato generico) l'ambito di operatività per l'accesso ai predetti servizi e funzionalità è limitato a quanto ricompreso dal delegante all'atto di conferimento della delega conformemente a quanto previsto nell'Allegato 5, fermo restando che in nessun caso il delegato accede ai dati soggetti a maggiore tutela, di cui all'art. 6 del decreto del Ministero della salute del 7 settembre 2023.
7. Il Dipartimento per la trasformazione digitale, nonché le Regioni e le Province autonome con riferimento agli ambiti di competenza, promuovono iniziative volte a favorire la corretta e uniforme classificazione dei Servizi in rete da parte delle pubbliche amministrazioni ai sensi del comma 5 del presente articolo.

Art. 10
(*Durata della delega*)

1. Il delegante, al momento del conferimento, definisce il periodo di validità della delega che, in ogni caso, non può essere superiore a due anni, decorsi i quali la delega non può più essere esercitata e deve essere nuovamente presentata. Il delegante può in ogni momento revocare la delega tramite le funzionalità rese disponibili dal Portale o recandosi presso il proprio comune di residenza.
2. Il delegato può rinunciare in qualsiasi momento alle deleghe precedentemente accettate utilizzando una specifica funzionalità resa disponibile nel Portale.
3. La delega dei tutori, curatori o amministratori di sostegno prevista dall'articolo 3, comma 2, lettera *d)*, cessa al momento della cessazione, per qualunque causa, della qualità di tutore,

curatore o amministratore di sostegno. La delega dei procuratori di cui all'articolo 5, comma 1, secondo periodo, cessa in caso di revoca o di estinzione della procura.

4. La delega dell'esercente la responsabilità genitoriale e del tutore del minore prevista dall'articolo 3, comma 2, lettera *c),* cessa al raggiungimento della maggiore età del minore stesso.
5. La delega è revocata automaticamente nel caso di esito negativo delle verifiche effettuate dal Gestore della Piattaforma di cui all'articolo 6, commi 5, 6 e 7 e all'articolo 7, comma 4.
6. La delega può essere altresì revocata su ordine dell'Autorità giudiziaria tramesso al Gestore della Piattaforma che provvede tempestivamente al suo annullamento.
7. La delega può essere nuovamente presentata anche prima della scadenza; in tale caso, il termine della durata di cui al comma 1, decorre dalla data della nuova presentazione e dalla medesima data, la delega precedente si intende sostituita.

Art. 11
(*Caratteristiche tecniche e requisiti di sicurezza*)

1. Le caratteristiche tecniche e i requisiti di sicurezza della Piattaforma sono descritti nell'Allegato 4 e sono individuati nel rispetto delle disposizioni in materia di cybersicurezza e, in particolare, di quelle previste dalla legge 28 giugno 2024, n. 90, e dal regolamento di cui al decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 27 giugno 2024, n. 21007.
2. Il Gestore della Piattaforma sviluppa l'infrastruttura tecnologica per l'attuazione dell'articolo 64-*ter* del CAD e del presente decreto, applicando i criteri di accessibilità di cui alla legge 9 gennaio 2004, n. 4, nel rispetto dei principi di usabilità, completezza di informazione, chiarezza del linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità e interoperabilità.
3. Le specifiche tecniche di integrazione sono descritte nell'Allegato 5. Al fine di assicurare l'allineamento costante dell'Allegato 5 alle continue evoluzioni tecnologiche o alla normativa di settore, eventuali successivi aggiornamenti delle specifiche tecniche in esso contenute sono adottati con decreto del Capo del Dipartimento per la trasformazione digitale, sentita l'Autorità Garante per la protezione dei dati personali, e sono pubblicati nell'apposita sezione dedicata del Portale. Col medesimo decreto sono aggiornati gli allegati da 1 a 4, ove necessario in conseguenza delle modifiche all'Allegato 5.
4. Le caratteristiche e le funzionalità delle deleghe sono altresì descritte in un manuale pubblicato sul Portale dove è pubblicata anche una guida utente.

Art. 12
(*Messa in funzione e malfunzionamenti*)

1. Prima della messa in funzione della Piattaforma, il Gestore della Piattaforma verifica ed attesta il suo corretto funzionamento tramite lo svolgimento di test. Il piano dei test, relativi anche alla sicurezza e alla performance della Piattaforma, è destinato alla totalità dei casi d'uso e delle funzionalità assegnate alla Piattaforma dall'articolo 64-*ter* del CAD e dal presente decreto.
2. Entro tre mesi dall'attestazione di cui al comma 2, i Gestori di identità digitale devono integrare i propri sistemi con la Piattaforma. La violazione di tale obbligo è punita ai sensi dell'articolo 18-*bis* del CAD.
3. Il malfunzionamento della Piattaforma dovuto a impedimenti tecnici, rilevati anche automaticamente dalla Piattaforma stessa, che non consentono la presentazione, registrazione o utilizzo della delega nonché il ripristino delle funzionalità, sono tempestivamente segnalate dal Gestore della Piattaforma nel Portale.

Art. 13
(*Trattamento dei dati personali*)

1. Il Gestore della Piattaforma è titolare del trattamento dei dati personali necessari per l'implementazione, la gestione e la manutenzione della Piattaforma.
2. L'accesso ai dati attraverso la piattaforma non modifica la disciplina relativa alla titolarità del trattamento.
3. Il comune di residenza è titolare del trattamento dei dati personali necessari per la presentazione della delega ai sensi dell'articolo 5 o necessari per il riscontro alla richiesta di accesso del cittadino ai sensi del comma 8 del medesimo articolo 5.
4. Qualora il Gestore della Piattaforma affidi a soggetti terzi, a qualunque titolo, lo svolgimento di attività inerenti al servizio di cui all'articolo 4, provvede alla loro nomina quali responsabili del trattamento ai sensi dell'articolo 28 del regolamento (UE) 2016/679, adottando misure idonee a garantire un'adeguata selezione e formazione degli operatori addetti al servizio e l'efficacia dei controlli di cui all'articolo 4, comma 4.

Art.14
(Piano di graduale rilascio dei servizi di presentazione della delega)

1. I servizi che consentono la presentazione della delega ai sensi del presente decreto sono resi progressivamente disponibili ai cittadini a decorrere dal 15 ottobre 2026, secondo i seguenti livelli di disponibilità:
    a. servizi che consentono la presentazione della delega secondo le previsioni dell'articolo 3, comma 2, lettere a) e c);
    b. servizi che consentono la presentazione della delega secondo le previsioni dell'articolo 3, comma 2, lettera b), e dell'articolo 4;

c. servizi che consentono la presentazione della delega secondo le previsioni dell'articolo 3, comma 2, lettere d) ed e), e dell'articolo 5.

2. Le date a decorrere dalle quali sono resi disponibili i servizi di cui al comma 1 sono pubblicate dal Gestore della Piattaforma sul Portale.
3. La data a decorrere dalla quale sono resi disponibili i servizi di cui al comma 1, lettera c), è definita dal Gestore della Piattaforma in accordo col Ministero della giustizia a seguito dell'adozione delle specifiche tecniche di cui all'articolo 7, comma 2.

Art. 15
(*Disposizioni finali*)

1. Gli allegati costituiscono parte integrante del presente decreto.
2. All'attuazione delle disposizioni di cui al presente decreto si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.
3. Il presente decreto è inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana.

Il Ministro della Giustizia

On. Carlo Nordio

NORDIO
CARLO
23.02.2026
11:29:35
UTC

Il Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri con delega all'innovazione tecnologica

Sen. Alessio Butti

BUTTI ALESSIO
PRESIDENZA
CONSIGLIO DEI
MINISTRI
20.02.2026 13:51:42
GMT+01:00

ALLEGATO 1

“Presentazione della delega con l'assistenza remota del Gestore della Piattaforma”

PIATTAFORMA DI GESTIONE DELEGHE

(Art. 4 - Presentazione della delega con l'assistenza remota del Gestore della Piattaforma)

La presentazione della delega di cui all'articolo 64-ter del CAD può essere effettuata mediante il servizio di assistenza remota (web meeting) del Gestore della Piattaforma, dai cittadini iscritti nell'ANPR di età pari o superiore ai 65 (sessantacinque) anni o in possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104.

Il servizio di assistenza remota prevede la presentazione della delega da remoto, tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196. Il Gestore della Piattaforma implementa un sistema che garantisce, preliminarmente all'instaurazione della sessione audio/video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente. Garantisce inoltre l'utilizzo di applicativi orientati all'usabilità e all'accessibilità da parte dell'utente.

La presentazione della delega mediante il servizio di assistenza remota prevede l'identificazione del soggetto delegante e delegato da remoto mediante una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento della delega nel rispetto delle seguenti condizioni:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione degli interlocutori 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 delegante, del delegato e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

Il Gestore della Piattaforma valuta la sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di presentazione della delega nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire le verifiche dell'identità dei soggetti e della volontà di delega.

L'operatore che acquisisce la delega effettua l'identificazione dei soggetti (delegante e delegato) accertandone l'identità tramite la verifica dei rispettivi documenti d'identità in corso di validità, purché muniti di fotografia recente riconoscibile e firma autografa e ne verifica il codice fiscale tramite la tessera sanitaria in corso di validità.

L'operatore può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza dei documenti presentati dai soggetti (delegante e delegato). La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca della delega con modalità crittografiche atte a garantirne l'accesso esclusivamente all'autorità giudiziaria, al gestore della piattaforma e ai soggetti delegante e delegato in caso di disconoscimento della stessa.

Il Gestore della Piattaforma deve richiedere il consenso al trattamento dei dati personali contenuti nelle riprese audio/video.

Il processo di erogazione del servizio è di seguito riportato:

1. Il cittadino delegante (di età pari o superiore ai 65 anni o in possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104) fornisce copia del documento d'identità, del proprio codice fiscale;
2. Il cittadino delegato:
    a. accede al Portale mediante l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo;

    b. carica sul Portale i documenti forniti dal delegante, la copia del documento d'identità, la copia del proprio codice fiscale.
3. La piattaforma (in modo automatico) verifica:
    a. che il delegante ed il delegato siano iscritti in ANPR;
    b. il possesso dei requisiti per l'erogazione del servizio da parte del delegante; per la verifica del possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 il Gestore verifica i relativi servizi INPS mediante PDND.
4. All'esito positivo delle sopracitate verifiche, Il cittadino delegato richiede un appuntamento per l'erogazione del servizio, selezionando una tra le date e orario disponibili;
5. La delega è registrata sul Portale a seguito della conclusione con esito positivo dell'erogazione del servizio e della successiva accettazione da parte del delegato.

L'erogazione del servizio, nella data e orario selezionati, deve essere condotta seguendo una procedura scritta e pubblicata dal Gestore della Piattaforma sul Portale ai Cittadini, che preveda almeno le seguenti attività:

- l'operatore effettua una video chiamata con delegato e delegante
- l'operatore**,** previa informativa, acquisisce dal delegante e delegato l'assenso alla videoregistrazione e alla sua conservazione. L'operatore informa che la videoregistrazione sarà conservata in modalità protetta fino ad 1 anno dopo la scadenza o revoca della delega, salvo contenziosi;
- l'operatore dichiara i propri dati identificativi;
- l'operatore verifica i documenti caricati;
- i soggetti delegante e delegato confermano le proprie generalità;
- il soggetto delegato dichiara di non possedere le seguenti qualifiche nei confronti del soggetto delegante:
    a. esercente la responsabilità genitoriale,
    b. tutore, curatore e amministratore di sostegno;
- il soggetto delegato conferma la data e l'ora della registrazione;
- il soggetto delegante esprime in piena consapevolezza la propria volontà di delega;
- l'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere, in generale, al delegato elencando le due opzioni di scelta possibili:
    a. Sola Consultazione;
    b. Completa
- il soggetto delegante comunica la sua scelta;
- l'operatore registra la volontà espressa dal delegante;
- l'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere al delegato, per Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina elencando tutte le scelte possibili e ricordando che è ammessa più di una scelta:
    - delega di tipo "0": non delegato;
    - delega di tipo "A": accesso completo dell'assistito delegante con i medesimi privilegi;
    - delega di tipo "B": consultazione dei dati e dei documenti relativi all'assistito;
    - delega di tipo "C": accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche;
    - delega di tipo "D": popolamento del taccuino personale dell'assistito.
- il soggetto delegante comunica la sua scelta;
- l'operatore registra opportunamente la volontà espressa dal delegante;
- i soggetti delegante e delegato forniscono opzionalmente i propri contatti telefonici o mail per la ricezione delle notifiche previste in merito l'utilizzo della delega;
- l'operatore chiede di inquadrare, fronte e retro, i documenti d'identità dei soggetti delegante e delegato, 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);

- l'operatore chiede di inquadrare, fronte e retro, la tessera sanitaria dei soggetti delegante e delegato, su cui è riportato il codice fiscale;
- l'operatore chiede ai soggetti di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;
- l'operatore riassume sinteticamente la volontà espressa dal soggetto delegante di conferire delega al soggetto delegato e raccoglie conferma dallo stesso.

ALLEGATO 2

“Formato standard per la presentazione della delega - Modello di attestazione medica”

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL MEDICO> codice fiscale <CF DEL MEDICO>,

nato/a il <DATA NASCITA DEL MEDICO> a <LUOGO DI NASCITA DEL MEDICO>,

e-mail <EMAIL DEL MEDICO >,

Recapito telefonico-<TELEFONO DEL MEDICO>,

in qualità di medico del Servizio Sanitario Nazionale (SSN), iscritto all'Ordine provinciale di <XXX>

con numero <XXX>

ATTESTO L'IMPOSSIBILITÀ DI

<NOME E COGNOME DEL DELEGANTE> codice fiscale <CF DELEGANTE>,

nato/a il <DATA DI NASCITA DEL DELEGANTE> a <LUOGO DI NASCITA DEL DELEGANTE>,

residente a <LUOGO DI RESIDENZA DEL DELEGANTE>,

documento d'identità n.ro <N.ro DOCUMENTO DELEGATO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

A RECARSI PRESSO IL PROPRIO COMUNE DI RESIDENZA

Luogo e data <LUOGO E DATA>

Timbro e firma del medico che rilascia l'attestazione

ALLEGATO 3

“Modulo per la richiesta di registrazione della delega presentata dal delegante o, nei casi tassativamente previsti, dal delegato presso il Comune di residenza del delegante.”

Modulo per la richiesta di registrazione della delega presentata dal delegante o, nei casi tassativamente previsti[1], dal delegato presso il Comune di residenza del delegante (art. 5, commi 1 e 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGANTE> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

e-mail <EMAIL>

DELEGA

<NOME E COGNOME DEL DELEGATO> codice fiscale <CF>, nato/a il <DATA DI NASCITA DEL> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

e-mail <EMAIL>

AD EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL SOTTOSCRITTO AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

La presente delega si intende (selezionare una delle opzioni seguenti):

- ☐ Sola Consultazione
- ☐ Completa

Per l'accesso a Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma nazionale di Telemedicina del sottoscritto, la tipologia di delega conferita è la seguente (selezionare una o più tipologie tra quelle contemplate all'art. 11 del D.M. Salute del 7 settembre 2023 (FSE 2.0), a seconda dell'ambito di operatività della delega:

- ☐ Tipo "0" [non delegato]
- ☐ Tipo "A" [accesso completo]
- ☐ Tipo "B" [consultazione dei dati e dei documenti relativi all'assistito delegante]
- ☐ Tipo "C" [accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche]
- ☐ Tipo "D" [popolamento del taccuino personale]

[1] Ai sensi dell'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, nel caso di cittadini allettati per lunga durata, ricoverati o impossibilitati per motivi sanitari a recarsi presso il Comune di residenza, la delega può essere presentata direttamente dal delegato.

Periodo di validità della delega[2]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca da parte del sottoscritto o rinuncia da parte del delegato.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA>

Firma del Delegante[3]

[2] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

[3] Apporre alla presenza dell'addetto al procedimento, fatta eccezione per le ipotesi di cui al citato art. 5, co.2.

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGANTE> codice fiscale <CF del delegante> - consapevole del fatto che le dichiarazioni mendaci, la falsità in atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. n. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del Delegante

Spazio riservato all'Ufficio.

(solo nel caso di delega presentata dal delegante ai sensi dell'art. 5, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe*)*

Le firme sono state apposte in mia presenza; ho identificato il sottoscrittore, che ha esibito un documento di riconoscimento in corso di validità.

Timbro e firma dell'addetto _

(solo nel caso di delega presentata dal delegato ai sensi dell'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe*)*

Attesto che la su esposta delega è stata presentata dal delegato ……. ……., che ho identificato previa esibizione di un documento di riconoscimento in corso di validità, il quale ha dichiarato che il delegante si trova in una condizione di impedimento temporaneo per ragioni di salute. La delega viene acquisita completa di copia del documento d'identità del delegante e di attestazione sanitaria.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note:

La delega deve essere sottoscritta dal delegante al momento della presentazione presso il Comune di residenza e alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità del delegante medesimo.

Solamente nei casi previsti all'art. 5, co. 2, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe (cittadini allettati per lunga durata, ricoverati o impossibilitati per motivi sanitari a recarsi presso il Comune di residenza) la delega potrà essere presentata dal delegato già sottoscritta dal delegante; in tal coso la delega dovrà essere corredata da:

1) copia del documento di identità del delegante;
2) copia di certificazione medica conforme all'allegato o certificazione rilasciata al delegante ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104.

Il delegato che presenta la delega dovrà in ogni caso esibire il proprio documento d'identità in corso di validità all'addetto al procedimento.
In riferimento all'art. 11, del D.M. Salute del 7 settembre 2023 (FSE 2.0), viene di seguito riportato il contenuto del comma *12:*

l'ambito di operatività della delega è ricompreso tra i seguenti:
a) accesso completo in base al quale il delegato opera sul FSE dell'assistito delegante con i medesimi privilegi (consultazione dei dati e dei documenti relativi all'assistito, inserimento di dati e documenti nel taccuino personale dell'assistito, nonché' accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché' oscuramenti e relative revoche);
oppure, singolarmente o in combinazione tra loro:

b) consultazione dei dati e dei documenti relativi all'assistito;
c) accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche;
d) inserimento di dati e documenti nel taccuino personale dell'assistito.

La delega può essere rilasciata a non più di due soggetti iscritti nell'ANPR (Anagrafe nazionale popolazione residente) ed è revocabile dal delegante in ogni momento tramite le funzionalità rese disponibili sul sito https://deleghedigitali.gov.it/ o recandosi presso il proprio Comune di residenza.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (art. 3, co.2 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal genitore esercente la responsabilità genitoriale o dal tutore presso il Comune di residenza del minore (art. 5, comma 6, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL GENITORE> codice fiscale <CF DEL GENITORE>, nato/a il <DATA NASCITA DEL GENITORE> a <LUOGO DI NASCITA DEL GENITORE>, documento d'identità n.ro <N.ro DOCUMENTO GENITORE> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL GENITORE>

RICHIEDE

la registrazione di una delega in qualità di esercente la responsabilità genitoriale sul minore <NOME E COGNOME DEL MINORE> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL MINORE AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

Periodo di validità della delega[4]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione per raggiungimento della maggiore età del minore.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del genitore o del tutore

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL GENITORE> codice fiscale <CF del genitore> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del genitore o del tutore

[4] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

Spazio riservato all'Ufficio.

Le firme sono stata apposte in mia presenza; ho identificato i sottoscrittori, che hanno esibito un documento di riconoscimento in corso di validità.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dall'esercente la responsabilità genitoriale o la tutela sul minore al momento della presentazione presso il Comune di residenza del minore medesimo.

È necessario esibire all'operatore un documento di riconoscimento in corso di validità.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal tutore, curatore o amministratore di sostegno presso il Comune di residenza del soggetto tutelato/inabilitato (art. 5, comma 6, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL TUTORE / CURATORE / AMMINISTRATORE DI SOSTEGNO> codice fiscale <CF>,

nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>,

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL>

RICHIEDE

la registrazione di una delega in qualità di TUTORE / CURATORE / AMMINISTRATORE DI SOSTEGNO di <NOME E COGNOME DEL TUTELATO/INABILITATO> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL TUTELATO/INABILITATO AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

Periodo di validità della delega[5]:

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione, per qualunque causa, della qualità di tutore/curatore/amministratore di sostegno.

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del tutore / curatore / amministratore di sostegno

[5] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

DICHIARAZIONE LIBERATORIA

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF del delegato> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n,. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del tutore / curatore / amministratore di sostegno

Spazio riservato all'Ufficio.

La firma è stata apposta in mia presenza; ho identificato il sottoscrittore che ha esibito un documento di riconoscimento.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dal tutore / curatore / amministratore di sostegno al momento della presentazione presso il Comune di residenza dell'interdetto/inabilitato/beneficiario alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità.

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

Modulo per la richiesta di registrazione della delega presentata dal delegato presso il Comune di residenza del delegante (art. 5, comma 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe)

Piattaforma Gestione Deleghe

(art. 64-ter Decreto legislativo 7 marzo 2005, n. 82)

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF>,

nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>,

documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>,

e-mail <EMAIL>

RICHIEDE

la registrazione di una delega in qualità di PROCURATORE di <NOME E COGNOME DEL SOGGETTO CHE HA CONFERITO LA PROCURA> codice fiscale <CF>, nato/a il <DATA NASCITA> a <LUOGO DI NASCITA>, documento d'identità n.ro <N.ro DOCUMENTO> rilasciato da <COMUNE DI RILASCIO> il <DATA RILASCIO> con scadenza il <DATA SCADENZA>

PER EFFETTUARE L'ACCESSO IN NOME E PER CONTO DEL RAPPRESENTATO…….. AI SERVIZI IN RETE EROGATI DALLE PUBBLICHE AMMINISTRAZIONI CHE RICHIEDONO L'IDENTIFICAZIONE INFORMATICA

La presente delega è valida a decorrere dal <GG/MM/AAAA INIZIO VALIDITÀ> fino al <GG/MM/AAAA FINE VALIDITÀ>, salvo revoca nei casi prescritti dalla normativa vigente, rinuncia o cessazione, per qualunque causa, della qualità di procuratore.

Periodo di validità della delega[6]:

Dichiara di aver preso visione delle informative privacy correlate all'utilizzo della "Piattaforma di gestione deleghe".

Data e ora <DATA E ORA> Firma del Delegato

DICHIARAZIONE LIBERATORIA

[6] Ai sensi dell'art. 10, co. 1, del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe, tale periodo non può essere superiore a due anni.

Il/La sottoscritto/a <NOME E COGNOME DEL DELEGATO> codice fiscale <CF del delegato> - consapevole del fatto che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dal Codice penale e dalle leggi speciali in materia e che la non veridicità del contenuto delle dichiarazioni rese comporterà, ai sensi dell'art. 75 del D.P.R. 445/2000, la decadenza dai benefici conseguenti all'attivazione della delega – dichiara sotto la propria responsabilità, ai sensi del citato D.P.R. n,. 445/2000, che la propria qualità di procuratore è tuttora sussistente e che non sono intervenute *medio tempore* modifiche o revoche.

Dichiara altresì, ai sensi del citato D.P.R. n. 445/2000, che quanto riportato nel presente modulo corrisponde alla sua effettiva volontà e non è stato estorto in alcun modo e che i fatti dichiarati rispondono al vero, esonerando sin d'ora l'operatore comunale addetto al procedimento, il Service Provider (Fornitore di servizi digitali) e il Gestore della Piattaforma di gestione deleghe da qualsivoglia responsabilità al riguardo, nei limiti previsti dalla vigente normativa applicabile.

Data e ora <DATA E ORA> Firma del Delegato

Spazio riservato all'Ufficio.

La firma è stata apposta in mia presenza; ho identificato il sottoscrittore che ha esibito un documento di riconoscimento.

Timbro e firma dell'addetto _

<STAMPA DELLE POLICY PRIVACY>

Note: la delega deve essere sottoscritta dal delegato al momento della presentazione presso il Comune di residenza dell'assistito alla presenza del dipendente comunale addetto al procedimento, previa esibizione di un documento di identità in corso di validità e di copia della procura notarile, generale o speciale, conferitagli

La registrazione della delega potrà essere effettuata solo all'esito positivo delle verifiche previste (artt. 3, co.2 e 7 del decreto recante la disciplina delle modalità di funzionamento della Piattaforma di gestione deleghe).

ALLEGATO 4

“Disciplinare tecnico”

DISCIPLINARE TECNICO

Caratteristiche tecniche e requisiti di sicurezza della piattaforma di gestione delle deleghe di cui all'articolo 64-ter del CAD

Definizioni

Si applicano le definizioni di cui al decreto cui questo allegato è parte integrante.

Introduzione

Il presente allegato definisce le caratteristiche tecniche e i requisiti di sicurezza della Piattaforma e le modalità operative per rendere disponibili la presentazione, accettazione e relativa registrazione della delega da parte dei cittadini iscritti nell'ANPR.

La Piattaforma è costituita dalle seguenti componenti:

a) Un'interfaccia web accessibile ai cittadini (Portale ai Cittadini);
b) Un'interfaccia web accessibile agli operatori comunali (Portale ai Comuni);
c) Un'interfaccia web accessibile agli operatori di backoffice (Portale di backoffice);
d) Un'interfaccia web accessibile agli operatori di helpdesk (Portale di helpdesk);
e) L'infrastruttura di backend della Piattaforma Deleghe (Backend).

1. 1 Portale ai Cittadini

La Piattaforma di Gestione Deleghe, mediante il "Portale ai cittadini", consente agli utenti autenticati di gestire in modo autonomo le deleghe digitali. Il "Portale Utente", in particolare, mette a disposizione degli utenti autenticati che intendono conferire una delega digitale (deleganti) le seguenti funzionalità:

- presentazione di una delega da parte del soggetto delegante;
- accettazione di una delega da parte del soggetto delegato;
- presentazione di una delega, da parte del soggetto delegato, ricevuta dal delegante tramite documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata e avanzata;
- presentazione di una delega in proprio favore da parte del soggetto delegato in qualità di esercente la responsabilità genitoriale o di tutore del minore;
- presentazione di una delega in proprio favore da parte del soggetto delegato in qualità di tutore, di curatore o di amministratore di sostegno del soggetto tutelato;
- presentazione di una delega in favore di soggetto terzo, presentata da parte del soggetto in qualità di esercente la responsabilità genitoriale, di tutore, di curatore o di amministratore di sostegno del soggetto tutelato o minore;
- richiesta di presentazione di una delega, da parte del soggetto delegato in videochiamata mediante il servizio di assistenza remota;
- revoca di una delega da parte del soggetto delegante;
- rinuncia di una delega da parte del soggetto delegato;
- visualizzazione delle deleghe inserite e relativi dettagli;
- visualizzazione delle richieste di utilizzo delle deleghe.

1.2. Portale ai Comuni

La Piattaforma di Gestione Deleghe, mediante il Portale rivolto ai Comuni, consente agli utenti autenticati addetti al procedimento di fruire delle seguenti funzionalità:

- inserimento di una delega presentata dal delegante, allegando copia su supporto informatico della documentazione presentata dallo stesso;

- inserimento di una delega presentata dal delegato procuratore, allegando copia della procura generale o speciale presentata dallo stesso;
- inserimento di una delega presentata dal delegato, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- inserimento della delega presentata dall'esercente la responsabilità genitoriale o tutore del minore, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- inserimento della delega presentata dal tutore, curatore dell'inabilitato e dall'amministratore di sostegno, allegando copia su supporto informatico della documentazione presentata dallo stesso;
- revoca di una delega da parte del soggetto delegante.
- rinuncia di una delega da parte di un soggetto delegato

1.3. Portale di backoffice

La Piattaforma di Gestione Deleghe, mediante il Portale di backoffice, deve consentire agli operatori di back office autenticati di fruire delle seguenti funzionalità:

- verifica documentale e delle sottoscrizioni delle deleghe presentate dal delegato mediante il Portale rivolto ai cittadini e successiva registrazione della relativa delega;
- verifica dell'autocertificazione attestante la responsabilità resa dal genitore;
- registrazione di una delega mediante il servizio di assistenza remota in videochiamata;
- revoca di una delega, su richiesta del delegante;
- revoca di una delega, su ordine dell'Autorità giudiziaria trasmesso al Gestore della Piattaforma.

1.4. Portale di helpdesk

La Piattaforma di Gestione Deleghe, mediante il Portale di helpdesk, deve consentire agli operatori di helpdesk autenticati di fornire supporto a Comuni e cittadini.

1.5. Backend

La Piattaforma di Gestione Deleghe, mediante il Backend, deve consentire le seguenti funzionalità:

- verifica dell'iscrizione in ANPR del delegante e del delegato mediante cooperazione con il sistema ANPR attraverso PDND;
- verifica della qualità di esercente la responsabilità genitoriale mediante cooperazione con il Ministero della Giustizia attraverso PDND;
- verifica della qualità di tutore, di curatore o di amministratore di sostegno mediante cooperazione con il Ministero della Giustizia attraverso PDND;
- verifica del possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 attraverso PDND;
- verifica dell'elenco dei soggetti deceduti per il blocco delle deleghe attive;
- verifica della decadenza o sospensione della responsabilità genitoriale o dell'avvenuta emancipazione del minore per il blocco delle deleghe attive;
- verifica della decadenza o sospensione della qualità di tutore, di curatore o di amministratore di sostegno, per il blocco delle deleghe attive;
- verifica di validità temporale della delega;
- verifica che non siano presenti più di due deleghe per delegante.
- verifica del numero massimo di 5 deleghe per soggetto delegato, escluso i casi di esercente responsabilità genitoriale e tutori, curatori o amministratori di sostegno nonché dai procuratori generali e speciali.

- La delega può essere nuovamente presentata anche prima della scadenza; in tale caso, il termine della durata di cui al comma 1, decorre dalla data della nuova presentazione e dalla medesima data, la delega precedente si intende sostituita.

2. Integrazione con basi dati nazionali

La Piattaforma di Gestione Deleghe abilita l'interoperabilità con i sistemi informativi e le banche dati nazionali al fine gestire le deleghe digitali.

L'interoperabilità con i sistemi informativi e le banche dati nazionali è volta all'implementazione delle seguenti verifiche e funzionalità:

- **Verifica dei soggetti deceduti:**
  La Piattaforma coopera con i servizi del sistema ANPR, tramite la PDND, al fine di procedere al blocco delle deleghe attive riferite a soggetti deceduti. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per tali soggetti.
- **Verifica dell'iscrizione in ANPR dei soggetti deleganti e delegati:**
  La Piattaforma coopera con i servizi del sistema ANPR, tramite la PDND, anche al fine di assicurare l'allineamento delle informazioni anagrafiche ai sensi dell'articolo 62, comma 5, del CAD quali, in particolare, quelle relative all'iscrizione del cittadino delegante e delegato nell'ANPR, all'identificativo univoco del cittadino (ID ANPR), al numero e data di scadenza della carta di identità e al domicilio digitale del cittadino ove presente.
- **Verifica di sussistenza della qualità di esercente la responsabilità genitoriale:**
  La Piattaforma coopera con i servizi del Ministero della Giustizia tramite la PDND, per le verifiche di sussistenza della qualità di esercente la responsabilità genitoriale. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata in favore di tali soggetti. In assenza dei suddetti servizi verranno utilizzati i servizi di verifica di maternità, paternità e stato di famiglia esposti da ANPR attraverso PDND.
- **Verifica di sussistenza della qualità di tutore, di curatore o di amministratore di sostegno:**
  La Piattaforma coopera con i servizi del Ministero della Giustizia, tramite la PDND, al fine di ricevere giornalmente i dati afferenti alle nuove nomine o variazioni della qualifica di tutore, di curatore o di amministratore di sostegno e dell'assenza di provvedimenti di sospensione o ablativi della responsabilità genitoriale, procedendo al blocco tempestivo delle deleghe attive. Tali dati sono conservati per il tempo strettamente necessario a eseguire la revoca della delega registrata per tali soggetti.
- **Verifica del possesso di certificazione rilasciata ai sensi dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104**:
  La Piattaforma coopera con i servizi dell'INPS, tramite la PDND, al fine di appurare il possesso, da parte del delegante, del requisito necessario per richiedere la creazione della delega tramite Assistenza Remota. Tali dati sono conservati per il tempo strettamente necessario a finalizzare la richiesta di appuntamento.

3. Servizi per la richiesta e il rilascio della delega

La richiesta di accesso ai servizi ai cittadini descritti dal presente decreto è possibile dall'area dedicata della piattaforma di gestione deleghe previa identificazione mediante le modalità di cui ai commi 2-quater e 2-nonies dell'art. 64 del CAD.

3.1 Creazione della delega

Un cittadino delegante richiede una delega a favore di un altro cittadino tramite "Portale ai Cittadini" (Art. 3, comma 2.a)

1. Il cittadino delegante accede al Portale e avvia la richiesta di delega;
2. Il Portale ai Cittadini verifica che il cittadino (delegante e delegato) sia iscritto su ANPR;
3. Il Portale ai Cittadini deve richiedere al delegante di effettuare le seguenti scelte:
    3.1. selezionare, per la delega generale, se quest'ultima deve essere:
        - Sola consultazione
        - Completa
    3.2. selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
        - delega di tipo "0": non delegato;
        - delega di tipo "A": accesso completo dell'assistito delegante con i medesimi privilegi;
        - delega di tipo "B": consultazione dei dati e dei documenti relativi all'assistito;
        - delega di tipo "C": accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonchè oscuramenti e relative revoche;
        - delega di tipo "D": popolamento del taccuino personale dell'assistito.
4. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega entro trenta giorni, confermando che agisce a titolo personale, senza finalità professionali o economiche (art.8, comma 2);
5. Il Portale registra la delega richiesta e accettata dal delegato.
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega

Un cittadino delegato registra una delega per conto di un altro cittadino tramite Portale ai Cittadini (Art. 3, comma 2.b)

1. Il cittadino delegante compila e sottoscrive, con firma digitale o altro tipo di firma elettronica qualificata o avanzata (realizzata ai sensi dell'articolo 16 del decreto del ministero dell'Interno 8 settembre 2022), il modulo fornito dal Portale e lo consegna al delegato in formato digitale;
2. Il cittadino delegato accede al Portale e carica i documenti forniti dal delegante confermando che agisce a titolo personale, senza finalità professionali o economiche (art.8, comma 2)
3. Il Portale Deleghe verifica che il cittadino (delegante e delegato) sia iscritto su ANPR;
4. Il Portale ai Cittadini deve richiedere al delegato di effettuare le seguenti scelte:
    4.1. selezionare, per la delega generale, se quest'ultima deve essere:
    - Sola consultazione
    - Completa
    4.2. selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
    - delega di tipo "0": non delegato;
    - delega di tipo "A": accesso completo dell'assistito delegante con i medesimi privilegi;

- delega di tipo “B”: consultazione dei dati e dei documenti relativi all’assistito;
- delega di tipo “C”: accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche;
- delega di tipo “D”: popolamento del taccuino personale dell’assistito.

5. L’operatore di backoffice verifica i documenti e la validità delle sottoscrizioni;
6. Il portale registra la delega richiesta;
7. Il cittadino delegato e il cittadino delegante ricevono la notifica di registrazione della delega;

Un cittadino esercente la responsabilità genitoriale registra una delega per un minore tramite Portale ai Cittadini (Art. 3, comma 2.c)

1. Il cittadino esercente la responsabilità genitoriale verso un minore accede al Portale e fa richiesta di registrazione della relativa delega;
2. Il Portale verifica che il cittadino esercente la responsabilità genitoriale e il minore siano iscritti su ANPR;
3. Il sistema interroga i servizi ANPR mediante PDND per la verifica dello stato di famiglia;
4. Il cittadino esercente la responsabilità genitoriale dichiara, ai sensi del DPR 445/2000 e s.m.i., la propria qualità di esercente la responsabilità genitoriale sul minore;
5. Il Portale registra la delega richiesta dal cittadino in quanto esercente la responsabilità genitoriale;
6. Il cittadino delegato riceve la notifica di registrazione della delega.

Nelle more della disponibilità dei servizi del Ministero di Giustizia:

1. Il cittadino accede al Portale Cittadini, dove prima di registrare la delega dichiara, ai sensi del DPR 445/2000 e s.m.i., la propria qualità di esercente la responsabilità genitoriale sul minore;
2. Il Portale verifica tramite i servizi di ANPR in PDND che il cittadino e il minore siano iscritti su ANPR;
3. Il Portale verifica la maternità e/o paternità e lo stato di famiglia richiamando specifici servizi su ANPR;
4. Il Portale verifica l’assenza di provvedimenti di sospensione o ablativi della responsabilità genitoriale;
5. Il Portale registra la delega richiesta dal cittadino in quanto esercente la responsabilità genitoriale.

Quando la delega è presentata dagli esercenti la responsabilità genitoriale si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo “A”, accesso completo dell’assistito delegante con i medesimi privilegi;

Un cittadino tutore, curatore dell’inabilitato e amministratore di sostegno registra una delega ad operare per conto del tutelato, dell’inabilitato e beneficiario dell’amministrazione di sostegno tramite Portale ai Cittadini (Art. 3, comma 2.d)

1. Il cittadino tutore, curatore o amministratore di sostegno di un altro cittadino accede al Portale e registra la relativa delega;
2. Il Portale verifica che il cittadino tutore, curatore o amministratore di sostegno e il tutelato siano iscritti su ANPR;
3. Il Portale verifica le informazioni tramite PDND nel dominio Giustizia;

4. Il Portale registra la delega richiesta dal cittadino in quanto tutore, curatore o amministratore di sostegno;
5. Il cittadino delegato riceve la notifica di registrazione della delega.

Quando la delega è presentata da tutori, curatori, amministratori di sostegno nonché dai procuratori generali si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo "A", accesso completo dell'assistito delegante con i medesimi privilegi;

Un cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell'inabilitato e l'amministratore di sostegno registra una delega per operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno in favore di un altro soggetto (Art. 3, comma 2.e)

1. Il cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell'inabilitato o l'amministratore di sostegno accede al Portale e presenta la delega ad operare per conto del minore, dell'interdetto, dell'inabilitato o del beneficiario dell'amministrazione di sostegno in favore di un altro soggetto;
2. Il Portale Deleghe verifica che le parti coinvolte (minore/interdetto/inabilitato, delegante, delegato) siano iscritti in ANPR;
3. Il Portale ai Cittadini deve richiedere al delegante di effettuare le seguenti scelte:
    3.1. selezionare, per la delega generale, se quest'ultima deve essere:
        - Sola consultazione
        - Completa
    3.2. selezionare per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina se la delega deve essere (possibilità di scelta multipla):
        - delega di tipo "0": non delegato;
        - delega di tipo "A": accesso completo dell'assistito delegante con i medesimi privilegi;
        - delega di tipo "B": consultazione dei dati e dei documenti relativi all'assistito;
        - delega di tipo "C": accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche;
        - delega di tipo "D": popolamento del taccuino personale dell'assistito.
4. Il Portale Deleghe verifica le informazioni tramite PDND nel dominio Giustizia;
5. Il Portale registra la delega all'accettazione del delegato.
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega.

Presentazione della delega con l'assistenza remota (web meeting) del Gestore della Piattaforma (Art. 4)

1. Il cittadino delegante (di età pari o superiore ai 65 anni o in possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104) fornisce copia del proprio documento d'identità, il codice fiscale e dichiarazione relativa al possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 (se applicabile);
2. Il cittadino delegato:
    2.1. accede al Portale mediante l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo;
    2.2. carica sul Portale i documenti forniti dal delegante, la copia della propria carta d'identità e la copia del proprio codice fiscale.

3. La piattaforma verifica:
    3.1. che il delegante ed il delegato siano iscritti in ANPR;
    3.2. il possesso dei requisiti per l'erogazione del servizio da parte del delegante; per la verifica del possesso di certificazione rilasciata ai sensi della dell'articolo 3, comma 3, della Legge 5 febbraio 1992, n. 104 il Gestore verifica i relativi servizi INPS mediante PDND;
4. All'esito positivo delle sopracitate verifiche, Il cittadino delegato richiede un appuntamento per l'erogazione del servizio, selezionando una tra le date e gli orari disponibili;
5. L'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere, in generale, al delegato elencando le due opzioni di scelta possibili:
    - Sola Consultazione;
    - Completa
6. Il soggetto delegante comunica la sua scelta;
7. L'operatore registra la volontà espressa dal delegante;
8. L'operatore richiede al delegante di esplicitare l'autorizzazione che vuole concedere al delegato, per Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina elencando tutte le scelte possibili e ricordando che è ammessa più di una scelta:
    - delega di tipo "0": non delegato;
    - delega di tipo "A": accesso completo dell'assistito delegante con i medesimi privilegi;
    - delega di tipo "B": consultazione dei dati e dei documenti relativi all'assistito;
    - delega di tipo "C": accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche;
    - delega di tipo "D": popolamento del taccuino personale dell'assistito.
9. Il soggetto delegante comunica la sua scelta;
10. L'operatore registra opportunamente la volontà espressa dal delegante;
11. La delega è registrata sul Portale a seguito della conclusione con esito positivo dell'erogazione del servizio di web meeting;
12. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Ulteriori dettagli riportati in Allegato 1.

<u>Un cittadino delegante presenta una delega a favore di un altro soggetto tramite sportello presso il proprio comune di residenza (Art. 5, comma 1)</u>

1. Il cittadino delegante presenta allo sportello comunale il modulo delega;
2. L'impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
4. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega;
5. Il Portale registra la delega all'accettazione del delegato;
6. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

<u>Un cittadino delegato in possesso di una procura generale o speciale richiede una delega tramite lo sportello presso il comune di residenza del delegante (Art. 5, comma 1)</u>

1. Un cittadino delegato esibisce allo sportello comunale copia della procura generale o speciale e copia del proprio documento di identità;

2. L’impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
4. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Quando la delega è presentata dai procuratori generali si considera sempre automaticamente Completa e per il Fascicolo Sanitario Elettronico, Ecosistema Dati Sanitari, Piattaforma Nazionale di Telemedicina si considera sempre automaticamente di tipo “A”, accesso completo dell’assistito delegante con i medesimi privilegi;

Un cittadino delegato presenta una delega in proprio favore tramite sportello presso il comune di residenza del delegante (Art. 5, comma 2)

1. Il cittadino delegante consegna al delegato il modulo delega firmato e il certificato medico;
2. Il cittadino delegato presenta allo sportello comunale il modulo delega e il certificato medico;
3. L’impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
4. Il Portale verifica che i cittadini (delegante e delegato) siano iscritti su ANPR;
5. Il cittadino delegato riceve una notifica, accede al Portale e accetta la delega;
6. Il Portale registra la delega all’accettazione del delegato;
7. Il cittadino delegato e il delegante ricevono la notifica di registrazione della delega;

Un cittadino esercente la responsabilità genitoriale, tutore, curatore dell’inabilitato e amministratore di sostegno presenta una delega per operare per conto del minore, dell’interdetto, dell’inabilitato o del beneficiario dell’amministrazione di sostegno tramite sportello presso il comune di residenza (Art. 5, comma 6)

1. Il cittadino genitore esercente la responsabilità genitoriale, il tutore, il curatore dell’inabilitato o l’amministratore di sostegno presenta allo sportello comunale il modulo delega;
2. L’impiegato comunale verifica i documenti e le sottoscrizioni, quindi carica la richiesta con i relativi allegati utilizzando il portale dedicato ai comuni;
3. Il Portale Deleghe verifica le informazioni tramite PDND nel dominio Giustizia;
4. Il Portale registra la delega;
5. Il cittadino delegato riceve la notifica di registrazione della delega.

3.2 Utilizzo della delega

In fase di accesso da parte del delegato ai servizi in rete erogati dalle Pubbliche Amministrazioni che richiedono l’identificazione informatica, il Gestore dell’identità digitale (IdP) abilita la possibilità per il cittadino di scegliere se operare per conto di un soggetto delegante.
Nel caso in cui il cittadino scelga di operare per conto di un soggetto delegante l’IdP interroga la Piattaforma per verificare la sussistenza di una delega valida.
Se la risposta della Piattaforma è positiva, l’IdP consente l’accesso al delegato per conto del delegante ed invia al SP l’informazione che l’accesso avviene mediante delega.
L’IdP, inoltre, deve trasferire al SP l’informazione se la delega è in Sola consultazione o Completa e nei soli casi in cui il SP gestisca il Fascicolo Sanitario Elettronico, l’Ecosistema Dati Sanitari, la Piattaforma Nazionale di Telemedicina l’IdP deve trasferire anche l’informazione relativa al tipo di delega concesso (0/A/B/C/D).

Utilizzo della delega

Di seguito si dettagliano gli step necessari all'utilizzo della delega.

1. Il cittadino accede ad un servizio in rete erogato da una Pubblica Amministrazione (SP);
2. Il cittadino in fase di autenticazione esprime la volontà di operare come delegato;
3. L'IdP, su richiesta del cittadino delegato, effettuata il reindirizzamento su una pagina della Piattaforma;
4. La Piattaforma, con opportune misure di sicurezza, recupera le deleghe conferite al delegato, effettua le verifiche di validità previste (quali l'esistenza in vita del delegante, la verifica di sussistenza della qualità di esercente la responsabilità genitoriale o la verifica di sussistenza della qualità di tutore, di curatore o di amministratore di sostegno) e mostra l'elenco delle deleghe valide all'utente;
5. Il delegato seleziona la delega, esprime il consenso ad inviare all'IdP i dati necessari all'accesso mediante delega;
6. Il cittadino delegante, laddove previsto dal DPCM, riceve una notifica di utilizzo della delega da parte del delegato;
7. L'IdP riceve dalla Piattaforma i dati necessari o restituisce un errore nei casi previsti;
8. L'IdP presenta i dati del delegante, sostituiti a quelli del delegato, in fase di autenticazione al servizio erogato dal SP.

3.3 Revoca e rinuncia della delega

Il delegante può in ogni momento revocare la delega tramite le funzionalità rese disponibili dal Portale o recandosi presso il proprio comune di residenza.
Il delegato può rinunciare in qualsiasi momento alle deleghe precedentemente accettate utilizzando una specifica funzionalità resa disponibile nel Portale.
La delega è revocata automaticamente nel caso di esito negativo delle seguenti verifiche:

- Sussistenza delle qualità di esercente la responsabilità genitoriale (dato del Ministero Giustizia) o emancipazione del minore (dato presente in ANPR);
- Sussistenza delle qualità di tutore, di curatore o di amministratore di sostegno (dato del Ministero Giustizia);
- Decesso del delegante/delegato (Servizio di "esistenza in vita" di ANPR).

La delega viene inoltre revocata su richiesta dell'Autorità Giudiziaria.

4. Misure di sicurezza

Il presente paragrafo elenca le misure di sicurezza tecniche e organizzative messe in atto dal Gestore della piattaforma.

Le misure di sicurezza sono individuate nel rispetto delle disposizioni in materia di cybersicurezza e, in particolare, di quelle previste dalla legge 28 giugno 2024, n. 90, e dal regolamento di cui al decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 27 giugno 2024, n. 21007.

Le misure di sicurezza sono organizzate nelle funzioni, categorie e sottocategorie del "Framework nazionale per la cybersecurity e la data protection", edizione 2019.

Per ogni misura è fornito un elenco di punti che rappresentano i requisiti dell'implementazione minima attesa.

Il termine "soggetto", ovunque ricorra nel presente paragrafo, è da intendersi riferito al Gestore della piattaforma.

Ad eccezione dell'organizzazione di cybersecurity (definita alla misura ID.AM-6), il termine "organizzazione", ovunque ricorra nel presente paragrafo, è da intendersi riferito almeno ai sistemi informativi e di rete tramite i quali è realizzata la piattaforma, nonché alle strutture e al personale del Gestore della piattaforma a vario titolo coinvolti nell'ambito dello sviluppo e della gestione della piattaforma.

4.1 Identificazione

4.1.1 Gestione degli asset (Asset Management) (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facility necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.

4.1.1.1 ID.AM-1. Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione.

1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. L'accesso alla rete è consentito esclusivamente ai soli sistemi e apparati fisici approvati.

4.1.1.2 ID.AM-2. Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione.

1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.
2. L'installazione è consentita esclusivamente alle piattaforme e applicazioni software approvate.

4.1.1.3 ID.AM-3. I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati.

1. Tutti i flussi informativi tra i sistemi informativi e di rete dell'organizzazione e l'esterno sono identificati ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. Le comunicazioni sono consentite esclusivamente per i flussi informativi approvati.

4.1.1.4 ID.AM-6. Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).

1. È definita e resa nota alle articolazioni del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. All'interno dell'organizzazione di cui al punto 1, è istituita e resa nota alle articolazioni del soggetto la struttura responsabile per l'attuazione delle misure di sicurezza di cui al presente allegato.
3. Esiste un elenco del personale interno ed esterno dell'organizzazione di cui al punto 1, ivi incluso quello della struttura di cui al punto 2, avente specifici ruoli e responsabilità.

4.1.2 Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.

4.1.2.1 ID.GV-1. È identificata e resa nota una policy di cybersecurity.

1. Le politiche e i processi di cybersecurity sono definiti per almeno i seguenti ambiti:
   a) governo;
   b) gestione del rischio;
   c) gestione degli asset;
   d) gestione del rischio di cybersecurity della catena di approvvigionamento;
   e) gestione delle vulnerabilità;
   f) business continuity e disaster recovery;
   g) gestione delle identità digitali, autenticazione e controllo degli accessi;
   h) sicurezza dei dati;
   i) manutenzione e riparazione dei sistemi;
   j) protezione delle reti;

k) monitoraggio degli eventi di sicurezza;
l) risposta e ripristino agli incidenti;
m) formazione del personale.

2. Esiste un documento aggiornato che descrive le politiche di cybersecurity di cui al punto 1.
3. Esiste un documento aggiornato che descrive i processi di cybersecurity di cui al punto 1.
4. Le politiche e i processi di cui al punto 1 sono revisionati periodicamente e quando necessario.

4.1.2.2 ID.GV-4. La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.

1. Esiste un piano aggiornato per la gestione del rischio informatico.

4.1.3 Valutazione del rischio (Risk Assessment) (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.

4.1.3.1 ID.RA-1. Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, esiste un piano aggiornato che descrive l'insieme delle attività finalizzate all'identificazione delle vulnerabilità contenente almeno:
   a) le modalità per l'identificazione delle vulnerabilità;
   b) la pianificazione delle attività per l'identificazione delle vulnerabilità.
2. Sono eseguite periodicamente le attività per identificare le vulnerabilità di cui al punto 1 e predisposte apposite relazioni che contengono almeno:
   a) la descrizione generale delle attività effettuate e gli esiti delle stesse;
   b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza.

4.1.3.2 ID.RA-5. Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.

1. In accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4, esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno:
   a) l'identificazione del rischio;
   b) l'analisi del rischio;
   c) la ponderazione del rischio.
2. La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti.

4.1.3.3 ID.RA-6. Sono identificate e prioritizzate le risposte al rischio.

1. Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità.
2. Per il rischio residuo successivo al trattamento di cui al punto precedente, esiste un documento aggiornato che ne contiene la chiara descrizione. Il documento, con il quale si accetta il rischio residuo, è approvato da parte dei vertici del soggetto.

4.1.4 Gestione del rischio relativo alla catena di approvvigionamento (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di

approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

4.1.4.1 ID.SC-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione

1. Esiste un documento aggiornato di dettaglio, che descrive i processi di gestione del rischio inerente alla catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

4.1.4.2 ID.SC-2. I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber.

1. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi di information and communication technology (ICT).

4.1.4.3 ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber

1. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, con le misure di sicurezza applicate ai sistemi informativi e di rete della piattaforma. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.
2. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, con le misure di sicurezza applicate ai sistemi informativi e di rete della piattaforma. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.

4.1.4.4 ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1. Esiste un documento aggiornato recante, almeno, le modalità e la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.
2. Esiste una pianificazione aggiornata degli audit, verifiche, o altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.

4.2 Protezione

4.2.1 Gestione delle identità, autenticazione e controllo degli accessi (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

4.2.1.1 PR.AC-1. Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.

1. Salvo motivate e documentate ragioni di natura organizzativa o tecnica, le identità digitali sono individuali per gli utenti.
2. Le credenziali di accesso relative alle identità digitali sono robuste e aggiornate con una cadenza proporzionata ai privilegi dell'utenza.

3. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono verificate periodicamente le identità digitali e le credenziali di accesso, aggiornandole/revocandole in caso di variazioni (es. trasferimento o cessazione di personale).
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
6. In relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV 1.

4.2.1.2 PR.AC-3. L'accesso remoto alle risorse è amministrato.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono monitorati gli accessi da remoto ed esiste un log degli accessi da remoto eseguiti.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono definite le attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alla gestione degli accessi da remoto, esiste un documento aggiornato contenente almeno:
   a) l'elenco dei sistemi informativi e di rete ai quali è possibile accedere e le relative modalità;
   b) le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.1.3 PR.AC-4. I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

1. Le identità digitali sono assegnate in accordo al principio del privilegio minimo e nel rispetto del principio di separazione delle funzioni.
2. È assicurata la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.
3. Tutte le utenze con privilegi sono censite, approvate e utilizzate quando necessario registrando ogni accesso effettuato.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3
6. In relazione alla gestione dei diritti di accesso e alle relative autorizzazioni, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.1.4 PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)

1. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla misura ID.RA-5, contiene almeno:
    a) le modalità di autenticazione disponibili;
    b) la loro assegnazione alle categorie di transazioni.
2. La piattaforma consente l'accesso al delegante/delegato esclusivamente mediante un'autenticazione basata sull'identità digitale CIE e/o SPID con livello di sicurezza almeno significativo.

4.2.2 Consapevolezza e addestramento (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti

4.2.2.1 PR.AT-1. Tutti gli utenti sono informati e addestrati.

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita al personale dell'organizzazione e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco del personale che ha ricevuto la formazione e i relativi contenuti.

4.2.2.2 PR.AT-2. Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti.

4.2.3 Sicurezza dei dati (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.

4.2.3.1 PR.DS-1. I dati memorizzati sono protetti.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, salvo motivate e documentate ragioni di natura organizzativa o tecnica, sono utilizzati sistemi di cifratura dei dati, ivi compresi i dispositivi portatili e quelli removibili.
2. Sono impiegate tecniche di pseudonimizzazione dei dati personali.
3. Gli algoritmi e i parametri di cifratura e delle tecniche di pseudonimizzazione sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
6. In relazione alla memorizzazione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.3.2 PR.DS-2: I dati sono protetti durante la trasmissione

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, salvo motivate e documentate ragioni di natura organizzativa o tecnica, le comunicazioni, inclusi i flussi di cui alla misura ID.AM-3, sono cifrati con protocolli e algoritmi allo stato dell'arte.

2. Gli algoritmi e i parametri di cifratura delle comunicazioni sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
5. In relazione alla trasmissione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.3.3 PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni.

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
    a) l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni;
    b) le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;
    c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. I meccanismi di controllo dell'integrità dei dati di cui al punto 1, lettera a) sono conformi alle Linee guida funzioni crittografiche emanate da ACN.

4.2.3.4 PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione.

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
    a) l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata;
    b) le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione;
    c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4.2.4 Procedure e processi per la protezione delle informazioni (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset.

4.2.4.1 PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)

1. Sono definite, e documentate in un elenco, le configurazioni di riferimento sicure (*hardened*) per i sistemi IT.
2. Salvo motivate e documentate ragioni di natura organizzativa o tecnica, sono consentiti l'installazione e l'utilizzo delle sole configurazioni di cui al punto 1.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1e 2.

4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alle configurazioni di riferimento dei sistemi IT, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.4.2 PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).

1. La piattaforma è sviluppata secondo le linee guida di sicurezza nello sviluppo delle applicazioni dell'Agenzia per l'Italia Digitale e le migliori pratiche di riferimento.
2. Viene gestito il ciclo di vita della piattaforma e dei relativi sistemi informativi e di rete.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 2.

4.2.4.3 PR.IP-4. I backup delle informazioni sono eseguiti, amministrati e verificati.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono effettuati periodicamente i backup dei dati.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è assicurata la riservatezza delle informazioni contenute nei backup mediante cifratura.
3. Gli algoritmi e i parametri di cifratura impiegati per assicurare la riservatezza delle informazioni contenute nei backup di cui al punto 2 sono conformi alle Linee guida funzioni crittografiche emanate da ACN.
4. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.
5. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
6. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
7. In relazione al backup dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.4.4 PR.IP-9. Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.

1. Esistono piani aggiornati di continuità operativa/disaster recovery redatti in accordo alle relative politiche e ai relativi processi di cui alla misura ID.GV-1.

4.2.4.5 PR.IP-12. Viene sviluppato e implementato un piano di gestione delle vulnerabilità.

1. Le vulnerabilità emerse a seguito delle attività di cui al punto 2 della misura ID.RA-1 sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero, se del caso, accentando il rischio in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.

4. In relazione alla gestione delle vulnerabilità, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.5 Manutenzione (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.

4.2.5.1 PR.MA-1. La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5:
    a) i sistemi informativi e di rete sono aggiornati all'ultima versione raccomandata dal produttore;
    b) l'aggiornamento dei software, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla manutenzione e riparazione dei sistemi informativi e di rete, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.5.2 PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.
2. Tutti gli accessi eseguiti da remoto da personale di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.
3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, devono essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
6. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2, 3, 4 e 5.
7. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2, 3, 4 e 5.
8. In relazione alla manutenzione delle risorse e dei sistemi svolta da remoto, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.2.6 Tecnologie per la protezione (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

4.2.6.1 PR.PT-1. Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla conservazione dei log, con particolare riguardo all'integrità e alla disponibilità degli stessi, esiste un documento aggiornato contenente almeno le procedure, le metodologie e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.
5. **È registrata la motivazione dell'accesso ai log**

4.2.6.2 PR.PT-4. Le reti di comunicazione e controllo sono protette.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati i sistemi perimetrali, quali firewall, anche a livello applicativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1
4. In relazione alla protezione delle reti, esiste un documento aggiornato contenente almeno le procedure e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.3 Rilevamento

4.3.1 Monitoraggio continuo per la sicurezza (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

4.3.1.1 DE.CM-1. Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati sistemi di rilevamento delle intrusioni (intrusion detection systems - IDS).
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è monitorato il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali al fine di rilevare gli eventi di cybersecurity.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione al monitoraggio degli eventi di sicurezza, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.3.1.2 DE.CM-4. Il codice malevolo viene rilevato.

1. Sono presenti e aggiornati sistemi di protezione delle postazioni terminali.

2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.).
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. Esiste un documento aggiornato contenente almeno le procedure, le metodologie e le tecnologie impiegate per il rispetto delle politiche di cui al punto 3 e nell'ambito dei processi di cui al punto 4.

4.3.1.3 DE.CM-8. Vengono svolte scansioni per l'identificazione di vulnerabilità

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment prima della loro messa in esercizio.
2. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software.
3. Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.
4. Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.
5. Nell'ambito dei punti 1 e 2 è inclusa l'esecuzione di *Web application penetration test* (WAPT), per la verifica della presenza di eventuali vulnerabilità sul codice sorgente.
6. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2, 3, 4 e 5.
7. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2, 3, 4 e 5.
8. Esiste un documento aggiornato contenente almeno le procedure, le metodologie e le tecnologie impiegate per il rispetto delle politiche di cui al punto 6 e nell'ambito dei processi di cui al punto 7.

4.4 Risposta

4.4.1 Pianificazione della risposta (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

4.4.1.1.RS.RP-1. Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente.

1. Esiste un piano aggiornato di risposta agli incidenti all'interno del quale sono definiti almeno:

f) le articolazioni preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche;
g) le procedure per la notifica degli incidenti alle parti interessate;
h) le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

4.4.2 Analisi (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.

4.4.2.1 RS.AN-5. Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza).

1. In relazione alla gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia, nonché da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento, esiste un documento aggiornato contenente almeno:

i) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni;
j) le procedure, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui alla lettera a) nel rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV1.

4.5 Recupero

4.5.1 Pianificazione del ripristino (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

4.5.1.1 RC.RP-1. Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.

1. Esiste un piano di ripristino che prevede almeno, le procedure necessarie al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da un incidente di cybersecurity.

5. Accessibilità

La "Piattaforma di Gestione Deleghe" rispetta i criteri di accessibilità di cui alla legge 9 gennaio 2004, n. 4, nel rispetto dei principi di usabilità, completezza di informazione, chiarezza del linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità e interoperabilità.

ALLEGATO 5

“Profilo implementativo per il protocollo di utilizzo di una delega”

Dettaglio versione

Versione	Data	Modifiche	Autore
1.0	02/02/2026	Prima versione	IPZS

Introduzione

Questo allegato tecnico definisce un profilo implementativo dei protocolli di scambio tra Service Provider (SP), Identity Provider (IdP) e la Piattaforma Gestione Deleghe (PGD) per l'ottenimento da parte di un SP di una delega di un Utente.

Linguaggio Normativo e Convenzioni

Le parole chiave "DEVE" e "DEVONO", "NON DEVE" e "NON DEVONO", "RICHIEDE" e "RICHIESTO", "NON DEVE", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "PUÒ" e "OPZIONALE" nel presente documento devono essere interpretate come descritte nel [BCP14] [RFC2119] [RFC8174] quando e solo quando appaiono in maiuscolo.

Flusso High-Level

Nell'ambito dell'utilizzo della PGD sono coinvolti i seguenti attori principali:

- **Service Provider**: sistema che fornisce un servizio online della Pubblica Amministrazione come soggetto fruitore di una delega di un cittadino. È anche sinonimo di Relying Party;
- **Identity Provider**: sistema responsabile dell'identificazione del cittadino che si autentica al fine di accedere ad un servizio online del SP per conto di un soggetto terzo (delegante). Agisce come intermediario nella comunicazione tra SP e PGD;

- **Piattaforma Gestione Deleghe**: sistema che gestisce e fornisce le deleghe dei cittadini e interagisce con l'IdP per consentire al cittadino delegato di accedere per conto di un delegante ad un servizio online di un SP.



Gestione Abilitazione dei Service Provider

Per consentire la creazione e l'utilizzo di una delega per l'accesso ai servizi online di un SP, quest'ultimo DEVE effettuare una procedura tecnica di adesione a PGD secondo quanto definito nelle successive sezioni.

L'onboarding tecnico e la gestione operativa del SP su PGD richiedono l'autenticazione del SP tramite il meccanismo private_key_jwt (RFC 7523) e la verifica dell'autenticità tramite confronto con i metadata ufficiali pubblicati dalle fonti autoritative SPID/CIE (AgID e Ministero dell'Interno).

Panoramica del ciclo di vita e delle funzionalità di gestione degli SP

La PGD fornisce un insieme di funzionalità per gestire, la richiesta di abilitazione e il ciclo di vita dei SP abilitati. Il ciclo di vita degli SP si articola nelle seguenti fasi:

1. Onboarding Tecnico: Processo iniziale di abilitazione di un SP al sistema delle deleghe, definito nella sezione "Processo tecnico di abilitazione".
Al completamento dell'onboarding, la PGD rilascia al SP un **Trust Mark JWT**, un'attestazione firmata come prova dell'avvenuta abilitazione del SP a PGD, da conservare nei log come evidenza opponibile a terzi.

2. Operatività
Una volta completato l'onboarding, il SP è inserito nel Registro JWT degli SP abilitati, che viene reso disponibile pubblicamente dalla PGD. Durante le operazioni di autenticazione del cittadino ad un servizio online del SP, gli IdP verificano la presenza del SP nel registro e, se abilitato, mostrano al cittadino l'opzione di accesso con delega.

3. Gestione Continuativa
Durante la fase operativa, il SP può avere la necessità di effettuare operazioni amministrative sulla propria abilitazione. La PGD fornisce API REST dedicate per le seguenti operazioni di gestione:

- **Verifica Stato Abilitazione** (GET /pgd/sp/status): Consente al SP di interrogare lo stato corrente della propria abilitazione, la data di onboarding, e l'indirizzo email di contatto registrato.
- **Modifica Contatti** (PUT /pgd/sp/contact): Consente al SP di aggiornare l'indirizzo email di contatto (PEC o email istituzionale) utilizzato dalla PGD per le comunicazioni ufficiali.
- **Altre operazioni future**: La PGD si riserva di aggiungere ulteriori endpoint di gestione.

Tutti gli endpoint di gestione richiedono autenticazione del SP tramite il meccanismo private_key_jwt come definito nella sezione "Meccanismo di Autenticazione del SP".

4. Offboarding
Quando un SP desidera cessare l'utilizzo delle deleghe o viene revocato dalla PGD, viene avviato il processo di offboarding:

- **Offboarding Volontario**: Il SP richiede la rimozione dal registro PGD tramite endpoint dedicato (DELETE /pgd/sp/offboarding). La rimozione ha effetto entro massimo 24 ore (al successivo ciclo di generazione del Registro JWT).
- **Offboarding per Revoca**: La PGD revoca unilateralmente l'abilitazione di un SP (es. per violazioni, cessazione dei requisiti di PA, ecc.), rimuovendo l'identificativo del SP dal Registro JWT. In tal caso la PGD notifica il SP usando il canale di contatto registrato.

La revoca ha effetto immediato al successivo refresh del registro da parte degli IdP.
Dopo l'offboarding, il SP non può più utilizzare le API di gestione del ciclo di vita. Gli IdP non mostrano più l'opzione di accesso con delega poiché il SP non è più presente nel Registro JWT.
Il SP può richiedere un nuovo onboarding in qualsiasi momento, ripetendo l'intero processo tecnico di abilitazione.

La sezione seguente descrive in dettaglio il processo tecnico di onboarding, la struttura del Trust Mark JWT e del Registro JWT.
Le specifiche degli endpoint di onboarding/offboarding e di gestione del ciclo di vita dei SP, con il relativo meccanismo di client authentication (private_key_jwt), sono definite nella sezione “Endpoint SP-PGD”.

Processo tecnico di abilitazione

Il SP che vuol aderire alla PGD DEVE effettuare una richiesta di abilitazione all’endpoint /pgd/onboarding secondo quanto definito nella sezione “Endpoint di Onboarding”.

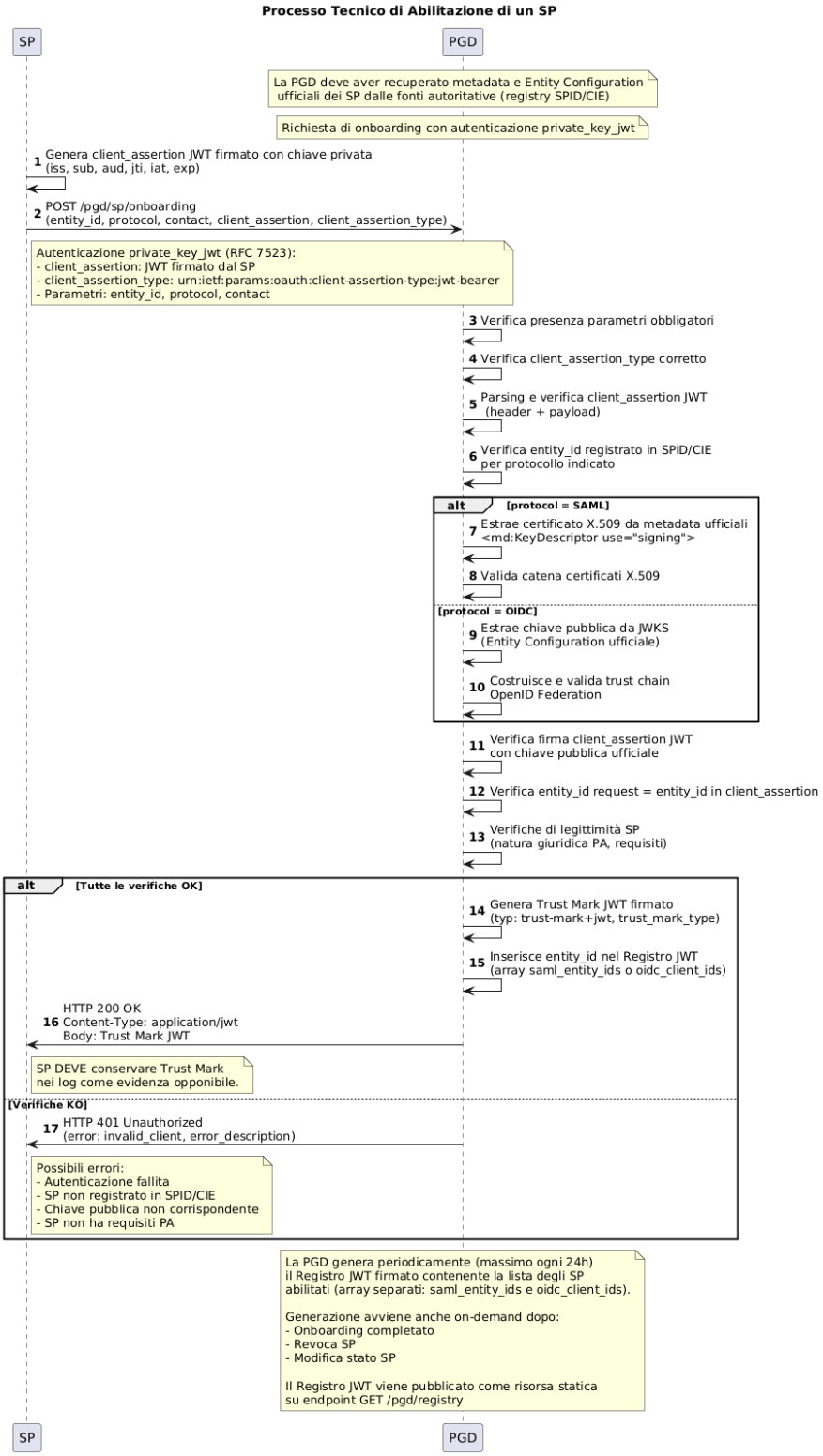


Figura 1 Processo tecnico di abilitazione di un SP

Come requisito preliminare la PGD DEVE ottenere tutti i metadata SAML registrati in SPID e CIE, anche a fronte di eventuali aggiornamenti.

Il SP DEVE autenticarsi usando il meccanismo di autenticazione definito nella sezione “Meccanismo di Autenticazione del SP” ed effettuare la richiesta di onboarding tramite l'endpoint POST /pgd/sp/onboarding.
La PGD DEVE effettuare le verifiche di sicurezza complete (vedi sezione “Processo di Verifica della PGD”) e, se tutte le verifiche hanno esito positivo, rilascia il Trust Mark (vedi sezione “Trust Mark”).

Il Trust Mark rilasciato dalla PGD viene utilizzato dal SP esclusivamente come evidenza opponibile a terzi dell'avvenuto onboarding.

Gli aggiornamenti che impattano i meccanismi di abilitazione dei Service Provider DEVONO essere comunicati con un preavviso minimo di 60 giorni agli IdP e ai SP già abilitati, al fine di consentire l'adeguamento dei sistemi.

Il Registro JWT dei SP Abilitati

Al termine del processo tecnico di abilitazione, la PGD DEVE inserire il SP all’interno di un registro centralizzato degli SP abilitati e DEVE rendere disponibile pubblicamente tale registro sotto forma di JWT firmato con validità massima di 24 ore.

Formato del Registro JWT

JWT Header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con “pgd-registry+jwt”.
- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma (vedi Sezione "Algoritmi Supportati").
- **kid**: [OBBLIGATORIO]. Stringa. Identificativo della chiave pubblica della PGD utilizzata per la firma in UUID v4.

JWT Payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo della PGD (es. https://deleghedigitali.gov.it).
- **iat**: [OBBLIGATORIO]. Intero. Timestamp Unix di emissione del registro.
- **exp**: [OBBLIGATORIO]. Intero. Timestamp Unix di scadenza del registro. La validità DEVE essere massimo 24 ore (exp - iat ≤ 86400).
- **saml_entity_ids**: [OBBLIGATORIO]. Array di stringhe. Lista degli entityID SAML degli SP abilitati al servizio deleghe. Può essere un array vuoto se non ci sono SP SAML abilitati
- **oidc_client_ids**: [OBBLIGATORIO]. Array di stringhe. Lista dei client_id OIDC degli SP abilitati al servizio deleghe. Può essere un array vuoto se non ci sono RP OIDC abilitati.

Esempio non normativo di Registro JWT:

```
{
```

```
  "typ": " pgd-registry+jwt",
  "alg": "ES256",
  "kid": " 3f231b99-f6d6-4518-07b9-08d0913fd28d"
}
.
{
  "iss": "https://deleghedigitali.gov.it",
  "iat": 1734960000,
  "exp": 1735046400,
  "saml_entity_ids": [
    "https://sp1.example.org",
    "https://sp3.gov.it/services/deleghe"
  ],
  "oidc_client_ids": [
    "https://sp2.example.gov.it"
  ]
}
}
```

Generazione e Aggiornamento del Registro

La PGD DEVE implementare un processo automatico di generazione del Registro JWT che viene eseguito:

- **Periodicamente**: Almeno ogni 24 ore (schedulazione automatica)
- **On-demand**: A seguito di eventi che modificano il registro degli SP (onboarding, revoca SP)

La generazione del Registro JWT DEVE essere attivata nei seguenti casi:

1. **Schedulazione temporale**: Job schedulato che viene eseguito almeno ogni 24 ore
2. **Evento onboarding SP**: Immediatamente dopo il completamento di un onboarding
3. **Evento revoca SP**: Immediatamente dopo la revoca di un SP

La PGD, durante il processo di generazione, DEVE:

1. **Estrarre SP attivi**: Recuperare dal database tutti gli SP con stato active (onboardatinon revocati)
2. **Separare per protocollo**: Organizzare gli SP in due array distinti:
    - saml_entity_ids: Array contenente gli entityID SAML degli SP abilitati
    - oidc_client_ids: Array contenente i client_id OIDC degli SP abilitati
3. **Generare timestamp**:
    - Claim iat: Timestamp Unix corrente (momento di generazione)
    - Claim exp: iat + 86400 (validità 24 ore)
4. **Costruire payload JWT**: Creare il payload del Registro JWT con i claim specificati nella sezione "Formato del Registro JWT"

5. **Firmare JWT**: Firmare il JWT con la chiave privata della PGD utilizzando l'algoritmo specificato nella sezione "Algoritmi Supportati"
6. **Includere kid**: Aggiungere nell'header JWT il claim kid contenente l'identificativo (UUID v4) della chiave pubblica utilizzata per la firma

Dopo la generazione del Registro JWT, la PGD DEVE pubblicarlo come risorsa statica per consentire la distribuzione efficiente agli IdP minimizzando il carico computazionale per richiesta, e renderlo disponibile tramite l'endpoint /pgd/registry (vedi sezione "Endpoint del Registro").

Nel caso di revoca di un SP, la PGD DEVE:
1. Eliminare l'identificativo del SP dal Registro (rimuovere l'entity_id dall'array saml_entity_ids o oidc_client_ids)
2. Rigenerare il Registro JWT
3. Pubblicare il nuovo Registro JWT come risorsa statica

La revoca ha effetto al successivo refresh del Registro da parte degli IdP (massimo 24 ore per refresh proattivo).

Verifica dell'abilitazione del SP da parte dell'IdP

La verifica dell'abilitazione del SP da parte degli IdP DEVE avvenire tramite il controllo della presenza dell'identificativo del SP nel Registro JWT che la PGD DEVE rendere disponibile tramite l'endpoint /pgd/registry.
All'accesso di uno specifico SP, l'IdP DEVE effettuare le verifiche riportate nella sezione "Endpoint del Registro" utilizzando il Registro JWT.
In caso di esito positivo di tutte le verifiche, dopo l'autenticazione dell'utente, l'IdP DEVE mostrare al cittadino l'opzione di accesso con delega.
In caso di fallimento di una qualsiasi verifica, l'IdP NON DEVE mostrare l'opzione di accesso con delega e DEVE procedere con il normale flusso di autenticazione senza delega.

Le specifiche tecniche complete dell'endpoint del registro sono definite nella sezione "Endpoint del Registro".

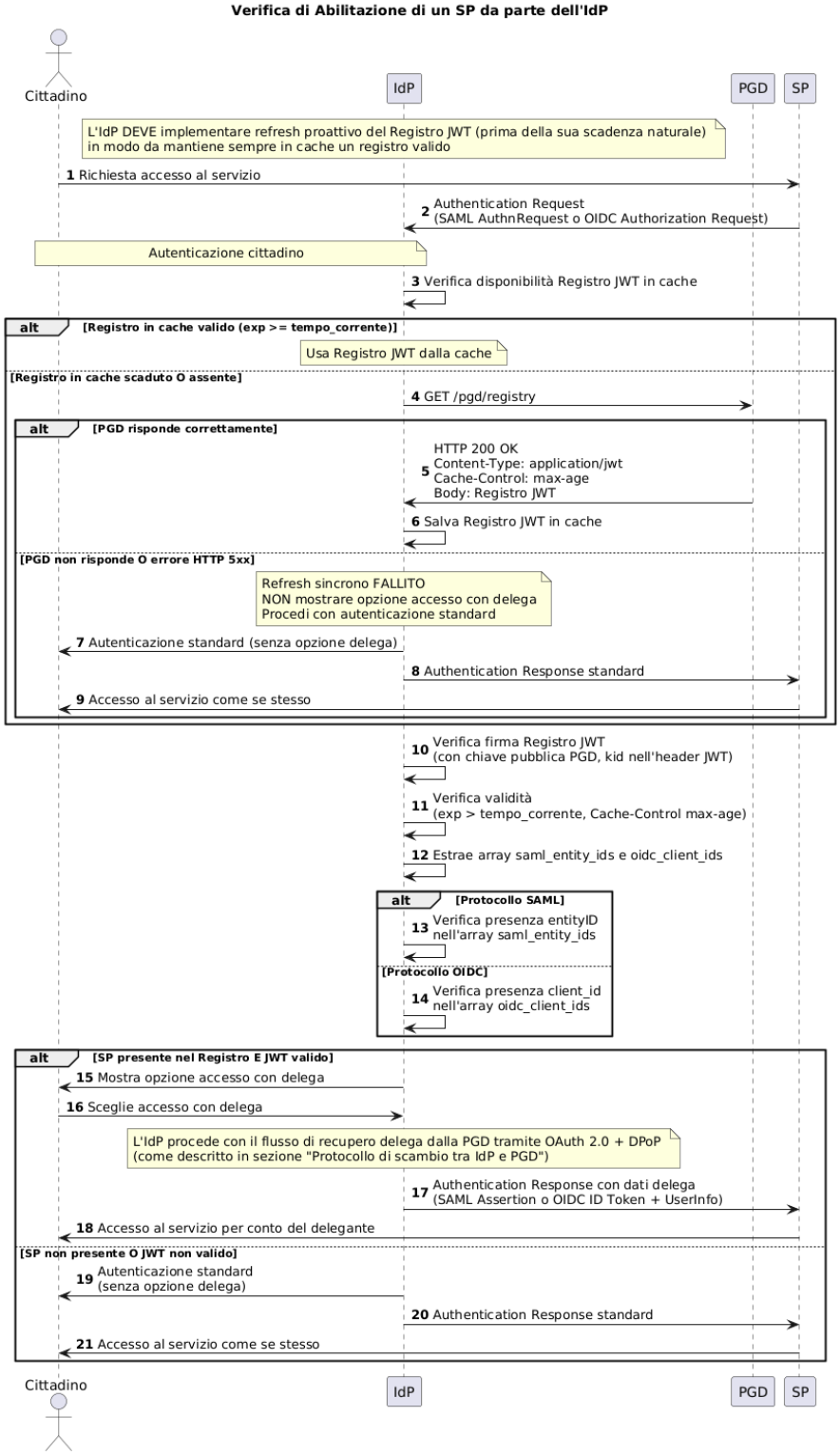


Figura 2 Verifica di abilitazione di un SP da parte di un IdP

Aggiornamento e Refresh del Registro

La PGD DEVE generare un nuovo Registro JWT ogni 24 ore al massimo, aggiornando automaticamente i timestamp *iat* ed *exp* e includendo l'elenco aggiornato degli SP abilitati (comprensivo di eventuali nuovi onboarding o revoche). Nel caso di revoca di un SP, la PGD DEVE eliminare l'identificativo del SP dal Registro.
Gli IdP DEVONO scaricare il nuovo Registro JWT almeno una volta ogni 24 ore per garantire l'aggiornamento delle abilitazioni. Gli IdP DEVONO implementare un meccanismo di caching locale del Registro JWT con refresh automatico prima della scadenza.

Endpoint SP-PGD

La PGD DEVE esporre endpoint HTTP dedicati per consentire agli SP di effettuare l'onboarding e gestire il proprio ciclo di vita. Tutti gli endpoint DEVONO soddisfare i seguenti requisiti di base:

- Utilizzo del protocollo HTTPS (TLS 1.2 o superiore).
- Autenticazione del SP tramite il meccanismo **private_key_jwt** secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP".

Endpoint	**Metodo**	**Descrizione**
/pgd/sp/onboarding	POST	Onboarding SP e inserimento nel registro dei SP abilitati
/pgd/sp/status	GET	Verifica stato abilitazione SP
/pgd/sp/contact	PUT	Modifica contatti SP
/pgd/sp/offboarding	DELETE	Offboarding SP dal registro dei SP abilitati

Meccanismo di Autenticazione del SP

Il meccanismo di autenticazione del SP DEVE essere conforme a quanto definito in OAuth 2.0 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC7523] e garantisce:

- **Proof-of-possession**: Il SP dimostra il possesso della chiave privata firmando un JWT (client_assertion) con la propria chiave privata
- **Non-repudiation**: Il JWT firmato costituisce evidenza crittografica dell'autenticazione non ripudiabile
- **Anti-impersonation**: La PGD verifica la firma del JWT utilizzando esclusivamente la chiave pubblica recuperata dai metadata ufficiali SPID/CIE pubblicati dalle fonti autoritative (AgID, Ministero dell'Interno), impedendo attacchi di impersonazione
- **Freshness**: Il JWT ha validità temporale limitata (claim exp, massimo 5 minuti) e contiene un identificativo univoco (claim jti) per prevenire attacchi replay

Struttura del client_assertion JWT

Il SP DEVE generare un JWT (client_assertion) con la seguente struttura:

Header:

- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma. È RACCOMANDATO ES256 (ECDSA con
  curva P-256 e SHA-256)
- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "pgd-registration-request+jwt"
- **kid**: [OBBLIGATORIO se non presente x5c]. Stringa. Key ID della chiave utilizzata per firmare il JWT. DEVE corrispondere al kid di una chiave pubblica presente nei metadata SPID/CIE del SP
- **x5c**: [OBBLIGATORIO se non presente kid]: Array di stringhe. Catena di certificati X.509 in formato Base64-encoded DER. Il primo certificato DEVE contenere la chiave pubblica utilizzata per firmare il JWT. I certificati successivi (se presenti) DEVONO formare la catena di certificazione.

Payload:

- iss: [OBBLIGATORIO]. Stringa. Issuer del JWT. DEVE essere l'entity_id del SP (entityID per SAML, client_id per OIDC)
- sub: [OBBLIGATORIO]. Stringa. Subject del JWT. DEVE essere l'entity_id del SP (stesso valore di iss)
- aud: [OBBLIGATORIO]. Stringa. Audience del JWT. DEVE essere l'identificativo della PGD (es. https://pgd.gov.it)
- jti: [OBBLIGATORIO]. Stringa. JWT ID. Identificativo univoco del JWT. È RACCOMANDATO utilizzare UUID v4.
- iat: [OBBLIGATORIO]. Numero (intero). Issued At. Timestamp Unix (secondi) di emissione del JWT
- exp: [OBBLIGATORIO]. Numero (intero). Expiration Time. Timestamp Unix (secondi) di scadenza del JWT. DEVE essere iat + massimo 300 secondi (5 minuti)

Esempio non normativo di client_assertion JWT:

```
{
"alg": "ES256",
"typ": "pgd-registration-request+jwt",
"kid": "NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs"
}.
{
"iss": "https://sp.example.org",
"sub": "https://sp.example.org",
"aud": "https://pgd.gov.it",
"jti": "a1b2c3d4-e5f6-4789-a012-3456789abcde",
"iat": 1734960000,
"exp": 1734960300
}
```

Invio della client_assertion

Il SP DEVE includere nella richiesta HTTP (body form-encoded) i seguenti parametri:

- client_assertion: [OBBLIGATORIO]. Stringa. Il JWT firmato (formato compatto JWT: header.payload.signature)
- client_assertion_type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con urn:ietf:params:oauth:client-assertion-type:jwt-bearer

Esempio non normativo di richiesta HTTP:

```
GET /pgd/sp/status HTTP/1.1
Host: pgd.gov.it
Content-Type: application/x-www-form-urlencoded
client_assertion=eyJhbGciOiJFUzI1NiIsInR5cCI6InBnZC1yZWdpc3RyYXRpb24tcmVxdWVzdCtqd3QiLCJraWQiOiJOemJMc1hoOHVEQ2NkLTZNTndYRjRXXzdub1dYRlpBZkhreFpzUkdDOVhzIn0.eyJpc3MiOiJodHRwczovL3NwLmV4YW1wbGUub3JnIiwic3ViIjoiaHR0cHM6Ly9zcC5leGFtcGxlLm9yZyIsImF1ZCI6Imh0dHBzOi8vcGdkLmdvdi5pdCIsImp0aSI6ImExYjJjM2Q0LWU1ZjYtNDc4OS1hMDEyLTM0NTY3ODlhYmNkZSIsImlhdCI6MTczNDk2MDAwMCwiZXhwIjoxNzM0OTYwMzAwfQ.signature&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer
```

Processo di Verifica della PGD

La PGD, a seguito della ricezione di una richiesta autenticata con private_key_jwt, DEVE effettuare le seguenti verifiche:

1. **Verifica formato client_assertion_type**: Verificare che il parametro client_assertion_type sia valorizzato con urn:ietf:params:oauth:client-assertion-type:jwt-bearer
2. **Parsing client_assertion JWT**: Decodificare header e payload del JWT (senza ancora verificare la firma)
3. **Verifica claim JWT obbligatori e validità temporale**: Verificare che:
    - iss e sub siano presenti e abbiano lo stesso valore

- aud sia presente e corrisponda all'identificativo della PGD (es. https://pgd.gov.it)
- iat ed exp siano presenti. Il valore dello iat NON DEVE essere non superiore all'istante in cui viene verificato il JWT.
- exp - iat <= 300 secondi (massimo 5 minuti di validità)
- il JWT non sia scaduto (exp > tempo corrente)
- jti sia presente e non sia già stato utilizzato in una richiesta precedente. La PGD PUÒ implementare una cache dei jti già utilizzati con TTL pari a 300 secondi (massima validità del JWT)

4. **Estrazione chiave pubblica del SP**: Estrarre dai metadata ufficiali la chiave pubblica corrispondente a quella specificata nell'header del client_assertion JWT:
   - **SAML**: Estrazione del certificato X.509 dalla sezione <md:KeyDescriptor use="signing">
   - **OIDC**: Estrazione della chiave pubblica dal JWKS pubblicato nell'Entity Configuration
5. **Verificare che la chiave pubblica estratta sia autentica (tramite la validazione della catena dei certificati x**.509 nel caso SAML, oppure tramite la costruzione e validazione della trust chain OpenID Federation nel caso OIDC)
6. **Verifica firma JWT (anti-impersonation)**: Verificare la firma del client_assertion JWT utilizzando **esclusivamente** la chiave pubblica estratta dai metadata ufficiali della fonte autoritativa.

Se tutte le verifiche hanno esito positivo, la PGD DEVE processare la richiesta.

Gestione errori
In caso di autenticazione non valida, la PGD DEVE rispondere con HTTP status code 401 Unauthorized e il seguente payload JSON:

```
{
"error": "invalid_client",
"error_description": "Invalid client authentication"
}
```

Gestione Chiavi per private_key_jwt

Il SP PUÒ utilizzare una chiave già presente nei propri metadata/Entity Configuration SPID/CIE per firmare il client_assertion JWT. Tuttavia, è RACCOMANDATO generare una nuova coppia di chiavi dedicata esclusivamente all'autenticazione verso PGD, garantendo separation of concerns e facilitando la rotazione indipendente.

Per SAML:
Se il SP genera nuove chiavi dedicate, DEVE:

1. Generare una nuova coppia di chiavi (RACCOMANDATO: ECDSA P-256)
2. Aggiungere la nuova chiave pubblica ai metadata SAML in <md:KeyDescriptor use="signing">
3. Risottomettere i metadata aggiornati ad AgID (per SPID) o Ministero dell'Interno (per CIE) seguendo le procedure previste dalle Regole Tecniche
4. Attendere la validazione e pubblicazione dei metadata aggiornati nei registri ufficiali
5. Solo dopo la pubblicazione dei metadata aggiornati, il SP PUÒ iniziare a utilizzare la nuova chiave per firmare i client_assertion JWT verso PGD

Per OIDC (OpenID Federation):
Se il SP genera nuove chiavi dedicate, DEVE:

1. Generare una nuova coppia di chiavi (RACCOMANDATO: ECDSA P-256)
2. Assegnare un kid descrittivo alla chiave
3. Aggiungere la nuova chiave pubblica al JWKS pubblicato nell'Entity Configuration
4. Aggiornare e ripubblicare l'Entity Configuration

In entrambi i casi, è RACCOMANDATO che il SP utilizzi un kid (Key ID) descrittivo per identificare la chiave dedicata a PGD.

Rotazione Chiavi

Il SP PUÒ ruotare le chiavi utilizzate per private_key_jwt in qualsiasi momento seguendo le procedure previste per l'aggiornamento dei metadata SPID/CIE.

Il SP DOVREBBE seguire la seguente procedura di rotazione:

1. Pubblicare la nuova chiave pubblica nei metadata SPID/CIE (mantenendo anche la vecchia)
2. Attendere la propagazione (per SAML: pubblicazione registry, per OIDC: immediato)
3. Iniziare a utilizzare la nuova chiave privata per firmare i client_assertion JWT
4. Dopo un periodo di overlap, rimuovere la vecchia chiave dai metadata

Questo approccio garantisce che la PGD possa validare sia i JWT firmati con la vecchia chiave (ancora in cache) che quelli firmati con la nuova chiave.

Endpoint di Onboarding

Richiesta HTTP

La richiesta HTTP di onboarding DEVE essere inviata usando il metodo HTTP POST.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con application/x-www-form-urlencoded

HTTP Request Body (form-encoded):

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC)
- protocol: [OBBLIGATORIO]: Stringa. Protocollo utilizzato dal SP nell'ambito delle federazioni CIE/SPID. Valori ammessi: saml, oidc
- contact: [OBBLIGATORIO]: Stringa. Indirizzo email di contatto del SP in formato PEC o email istituzionale della Pubblica Amministrazione
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT".
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo:

```
POST /pgd/sp/onboarding HTTP/1.1
Host: pgd.gov.it
Content-Type: application/x-www-form-urlencoded

entity_id= https%3A%2F%2Fsp.example.org&
protocol=saml&
contact=sp%40pec.example.it&
client_assertion=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBnZC1hdXRoLTIw
MjYtMDEifQ.eyJpc3MiOiJodHRwczovL3NwLmV4YW1wbGUub3JnIiwic3ViIjoiaHR0cHM6Ly9zcC
5leGFtcGxlLm9yZyIsImF1ZCI6Imh0dHBzOi8vcGdkLmdvdi5pdCIsImp0aSI6ImExYjJjM2Q0LWU
1ZjYtNDc4OS1hMDEyLTM0NTY3ODlhYmNkZSIsImlhdCI6MTczNDk2MDAwMCwiZXhwIjoxNzM0OTYw
MzAwfQ.signature&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
```

Verifiche della PGD

La PGD, a seguito della ricezione della richiesta, DEVE effettuare le seguenti verifiche:

- Verifica che siano presenti tutti i parametri obbligatori della richiesta HTTP.
- Verifica che l'entity_id inviato nella richiesta corrisponda a un SP registrato nella federazione CIE/SPID per il protocollo indicato nel parametro protocol. Tale verifica DEVE essere effettuata tramite i metadata ottenuti dai registri ufficiali CIE/SPID.
- Verificare che l'entity_id inviato nella richiesta HTTP corrisponda all'identificativo presente nella client_assertion.
- Verifica la corretta autenticazione del SP secondo quanto definito nella sezione "Meccanismo di Autenticazione del SP", in particolare nella sottosezione "Processo di Verifica della PGD".

Se tutte le verifiche hanno esito positivo, la PGD DEVE:

1. Generare un Trust Mark JWT firmato attestante l'abilitazione del SP
2. Inserire il SP nel Registro JWT degli SP abilitati (array saml_entity_ids o oidc_client_ids)
3. Registrare un evento di audit con, a titolo esemplificativo, entity_id, contact_email, timestamp, IP source.
4. Fornire una risposta HTTP con status code 200 contenente il Trust Mark.

Trust Mark

Il Trust Mark JWT DEVE contenere i seguenti claim:

Header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con trust-mark+jwt.
- **alg**: [OBBLIGATORIO]. Stringa. Algoritmo di firma (vedi Sezione "Algoritmi Supportati").
- **kid**: [OBBLIGATORIO]. Stringa. Identificativo della chiave pubblica della PGD utilizzata per la firma in UUID v4.

Payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo della PGD (es. https://pgd.gov.it).

- **sub**: [OBBLIGATORIO]. Stringa. Identificativo del SP (entityID SAML o client_id OIDC).
- **iat**: [OBBLIGATORIO]. Intero. Timestamp Unix di emissione del Trust Mark.
- exp: [OPZIONALE]. Intero. Timestamp Unix di scadenza del Trust Mark.
- **trust_mark_type**: [OBBLIGATORIO]. Stringa. Identificativo univoco del tipo di Trust Mark (es. https://pgd.gov.it/trustmark/delegation-enabled).

Risposta HTTP

La risposta HTTP DEVE avere il parametro Content-Type valorizzato con application/jwt e DEVE restituire nel body il Trust Mark JWT in formato compatto (header.payload.signature) come riportato nell'esempio non normativo seguente (Successo - 200 OK).

```
HTTP/1.1 200 OK
Content-Type: application/jwt
Cache-Control: no-store

eyJhbGciOiJFUzI1NiIsInR5cCI6InRydXN0LW1hcmsrand0Iiwia2lkIjoicGdkLXRtLWtleS0yM
DI2In0.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJzdWIiOiJodHRwczovL3NwLmV4YW1wbG
Uub3JnIiwidHJ1c3RfbWFya190eXBlIjoiaHR0cHM6Ly9wZ2QuZ292Lml0L3RydXN0bWFyay9kZWx
lZ2F0aW9uLWVuYWJsZWQiLCJpYXQiOjE3MzcxMTA0MDV9.MEUCIQCx2y3z4a5b6c7d8e9f0g1h2i3
j4k5l6m7n8o9p0q1r2s3tATBu4v5w6x7y8z9a0b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q
```

Trust Mark JWT decodificato:

```
{
  "alg": "ES256",
  "typ": "trust-mark+jwt",
  "kid": "pgd-tm-key-2026"
}.
{
  "iss": "https://pgd.gov.it",
  "sub": "https://sp.example.org",
  "trust_mark_type": "https://pgd.gov.it/trustmark/delegation-enabled",
  "iat": 1737110405
}
```

Gestione Errori

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Gestione Ciclo di Vita

Verifica Stato Abilitazione

La richiesta HTTP di verifica dello stato di adesione del SP DEVE essere inviata all'endpoint /pgd/sp/status usando il metodo GET. Questo endpoint consente al SP di verificare lo stato corrente della propria abilitazione.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con application/x-www-form-urlencoded

HTTP Request Body (form-encoded):

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC)
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT".
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
GET /pgd/sp/status HTTP/1.1
Host: pgd.gov.it
Content-Type: application/x-www-form-urlencoded

entity_id= https%3A%2F%2Fsp.example.org&
client_assertion=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBnZC1hdXRoLTIw
MjYtMDEifQ.eyJpc3MiOiJodHRwczovL3NwLmV4YW1wbGUub3JnIiwic3ViIjoiaHR0cHM6Ly9zcC
5leGFtcGxlLm9yZyIsImF1ZCI6Imh0dHBzOi8vcGdkLmdvdi5pdCIsImp0aSI6ImExYjJjM2Q0LWU
1ZjYtNDc4OS1hMDEyLTM0NTY3ODlhYmNkZSIsImlhdCI6MTczNDk2MDAwMCwiZXhwIjoxNzM0OTYw
MzAwfQ.signature&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
```

A seguito delle opportune verifiche (client authentication e verifiche di presenza dell'entity_id nel registro degli SP abilitati, PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC). DEVE corrispondere all'entity_id fornito nella richiesta.
- protocol: [OBBLIGATORIO]. Stringa. Protocollo utilizzato dal SP. Valori ammessi: saml, oidc.
- status: [OBBLIGATORIO]. Stringa. Stato corrente dell'abilitazione del SP. Valori ammessi: active (SP abilitato e presente nel Registro JWT), suspended (SP temporaneamente sospeso), revoked (SP revocato).

- onboarding_date: [OBBLIGATORIO]. Stringa. Data e ora di completamento dell'onboarding del SP. Formato: ISO 8601 UTC (es. 2025-01-14T10:30:00Z).
- contact: [OBBLIGATORIO]. Stringa. Indirizzo email di contatto del SP registrato in PGD (PEC o email istituzionale).

Di seguito un esempio non normativo della risposta HTTP.

HTTP Response (200 OK):

```
{
  "entity_id": "https://sp.example.org",
  "protocol":"saml",
  "status": "active",
  "onboarding_date":"2025-01-14T10:30:00Z",
  "contact": "admin@sp.example.org",
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Modifica Contatti

La richiesta HTTP di modifica dell'indirizzo email di contatto del SP DEVE essere inviata all'endpoint /pgd/sp/contact usando il metodo PUT. Questo endpoint consente al SP di aggiornare l'indirizzo email di contatto utilizzato dalla PGD per le comunicazioni ufficiali.

HTTP Request Headers:

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con application/x-www-form-urlencoded

HTTP Request Body (form-encoded):

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC)
- contact: [OBBLIGATORIO]. Stringa. Nuovo indirizzo email di contatto del SP in formato PEC o email istituzionale della Pubblica Amministrazione.
- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT".
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP:

```
PUT /pgd/sp/contact HTTP/1.1
Host: pgd.gov.it
Content-Type: application/x-www-form-urlencoded

entity_id=https%3A%2F%2Fsp.example.org&
```

```
contact =nuovo.contatto%40pec.example.it&
client_assertion=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBnZC1hdXRoLTIw
MjYtMDEifQ.eyJpc3MiOiJodHRwczovL3NwLmV4YW1wbGUub3JnIiwic3ViIjoiaHR0cHM6Ly9zcC
5leGFtcGxlLm9yZyIsImF1ZCI6Imh0dHBzOi8vcGdkLmdvdi5pdCIsImp0aSI6ImIxYzJkM2U0LWY
1ZzYtNDc4OS1iMDEyLTM0NTY3ODlhYmNkZiIsImlhdCI6MTczNDk2MDAwMCwiZXhwIjoxNzM0OTYw
MzAwfQ.signature&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
```

A seguito delle opportune verifiche (client authentication, verifiche di presenza dell'entity_id nel registro degli SP abilitati e validità del formato email), PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC). DEVE corrispondere all'entity_id fornito nella richiesta.
- contact: [OBBLIGATORIO]. Stringa. Nuovo indirizzo email di contatto del SP aggiornato con successo.
- updated_at: [OBBLIGATORIO]. Stringa. Data e ora dell'aggiornamento. Formato: ISO 8601 UTC (es. 2026-01-17T12:15:30Z).

Di seguito un esempio non normativo della risposta HTTP. HTTP Response (200 OK):

```
{
  "entity_id": "https://sp.example.org",
  "contact_email": "nuovo.contatto@pec.example.it",
  "updated_at": "2026-01-17T12:15:30Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Endpoint di Offboarding

La richiesta HTTP di offboarding (rimozione dal registro PGD) DEVE essere inviata all'endpoint /pgd/sp/offboarding usando il metodo DELETE. Questo endpoint consente al SP di richiedere volontariamente la rimozione della propria abilitazione al sistema delle deleghe.

HTTP Request Headers

- Content-Type: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con application/x-www-form-urlencoded

HTTP Request Body (form-encoded)

- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP (entityID per SAML, client_id per OIDC)

- client_assertion: [OBBLIGATORIO]. Stringa. JWT firmato dal SP con la propria chiave privata per l'autenticazione. Il JWT DEVE essere conforme a quanto definito nella sezione "Struttura del client_assertion JWT".
- client_assertion_type: [OBBLIGATORIO]. Stringa. Come definito nella sezione "Meccanismo di Autenticazione del SP".

Esempio non normativo della richiesta HTTP

```
DELETE /pgd/sp/offboarding HTTP/1.1
Host: pgd.gov.it
Content-Type: application/x-www-form-urlencoded

entity_id=https%3A%2F%2Fsp.example.org&
client_assertion=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBnZC1hdXRoLTIw
MjYtMDEifQ.eyJpc3MiOiJodHRwczovL3NwLmV4YW1wbGUub3JnIiwic3ViIjoiaHR0cHM6Ly9zcC
5leGFtcGxlLm9yZyIsImF1ZCI6Imh0dHBzOi8vcGdkLmdvdi5pdCIsImp0aSI6ImMxZDJlM2Y0LWc
1aDYtNDc4OS1jMDEyLTM0NTY3ODlhYmNkZyIsImlhdCI6MTczNDk2MDAwMCwiZXhwIjoxNzM0OTYw
MzAwfQ.signature&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
```

Processo di verifica della PGD

La PGD, a seguito della ricezione della richiesta, DEVE effettuare le seguenti verifiche:

1. Verificare l'autenticazione del SP tramite private_key_jwt (come definito nella sezione "Meccanismo di Autenticazione del SP")
2. Verificare che l'entity_id nel claim iss/sub del client_assertion corrisponda all'entity_id specificato nel body
3. Verificare che il SP sia attualmente abilitato nel registro PGD

Se tutte le verifiche hanno esito positivo, la PGD DEVE:

1. Marcare il SP come "in offboarding" con timestamp della richiesta
2. Programmare la rimozione dell'identificativo del SP dal Registro JWT (entro massimo 24 ore)
3. Registrare un evento di audit con: entity_id, timestamp, IP source
4. Fornire una risposta HTTP con status code 200 e Content-Type application/json

HTTP Response (200 OK)

A seguito delle opportune verifiche, PGD DEVE fornire una risposta HTTP con status code 200 e Content-Type application/json come di seguito definito.

- status: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con offboarded
- entity_id: [OBBLIGATORIO]. Stringa. Identificativo univoco del SP rimosso dal registro. DEVE corrispondere all'entity_id fornito nella richiesta.

- offboarding_date: [OBBLIGATORIO]. Stringa. Data e ora di ricezione della richiesta di offboarding. Formato: ISO 8601 UTC (es. 2026-01-17T16:00:00Z).

Di seguito un esempio non normativo della risposta HTTP.

```
{
  "status": "offboarded",
  "entity_id": "https://sp.example.org",
  "offboarding_date": "2026-01-17T16:00:00Z"
}
```

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Protocolli di comunicazione

Nelle sezioni seguenti viene dettagliato l'intero protocollo di comunicazione tra i vari attori del sistema che prevede, in particolare, le seguenti macro-fasi:

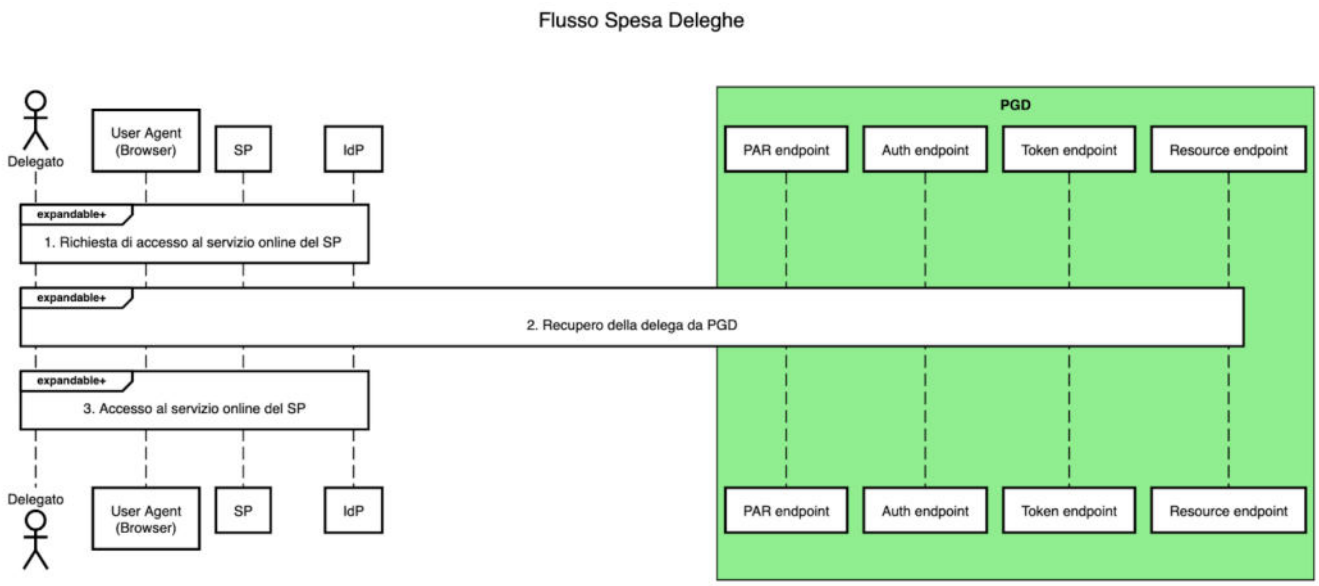
1. Richiesta di accesso al servizio online di un SP;
2. Recupero delle delega da PGD;
3. Accesso al servizio online del SP.

Le fasi 1) e 3) sono dettagliate nella Sezione “Protocollo di scambio tra SP e IdP”.
Il protocollo di scambio relativo alla fase 2) è descritto nella Sezione “Protocollo di scambio tra IdP e PGD”.

In particolare, quest'ultimo protocollo fornisce tutti gli strumenti utili a mitigare i seguenti attacchi:

- **MiTM (Man in the Middle):** Un attaccante si posiziona tra due parti comunicanti intercettando e potenzialmente modificando il traffico. Il protocollo mitiga questo attraverso l'uso di Proof of Possession che lega il token al possessore originale della richiesta di autenticazione, utilizza Client Assertion con JWT firmati per autenticare le richieste tra componenti e richiede un canale TLS esplicito per tutti gli endpoint;
- **Replay Attack**: L'attaccante cattura una comunicazione valida e la ri-trasmette in un secondo momento per replicare un'azione autorizzata. La mitigazione avviene tramite l'inclusione del parametro "jti" (JWT ID) univoco in ogni token e l'uso di parametri temporali "iat", "exp", "nbf" in tutti i JWT;
- **Malicious Administrator:** Un amministratore con privilegi elevati abusa del proprio accesso per compromettere il sistema. Il protocollo richiede l’inserimento di un OTP da parte del delegato durante il processo di utilizzo della delega;
- **Token Theft**: Un attaccante riesce a rubare un token di accesso valido e tenta di utilizzarlo. La mitigazione è effettuata attraverso il binding del token al client specifico tramite DPoP, la verifica della Proof of Possession per ogni richiesta protetta e la limitazione dello scope dei token alle sole operazioni di delega;
- **CSRF (Cross-Site Request Forgery)**: Un attaccante inganna un utente autenticato per fargli eseguire azioni non intenzionali. Il protocollo mitiga questo attraverso l'uso obbligatorio del parametro “state” nelle richieste di autorizzazione, la verifica della corrispondenza dello “state” tra richiesta e risposta, e l'obbligo di generare valori “state” casuali con entropia sufficiente (minimo 32 caratteri).
- **Mix-Up Attack**: Un attaccante inganna l'applicazione facendole scambiare informazioni sensibili con un server di identità malevolo mentre l'utente si autentica correttamente con un provider legittimo. Il protocollo mitiga questo attacco introducendo l’identificativo univoco della PGD nella Authorization Response richiedendo che l’IdP verifichi che tutte le richieste del flusso di autenticazione siano correttamente dirette alla PGD, confrontando gli identificativi univoci ad ogni passo.

Inoltre, il protocollo mitiga potenziali rischi di privacy limitando l'accesso dell'IdP alla sola delega selezionata dall'utente (e non all'intera lista delle deleghe a lui assegnate), e, in ogni caso, solo a seguito di un esplicito consenso dell’utente a comunicare tali dati all'IdP.
Segue il diagramma di alto livello del protocollo.



Nelle interazioni tra Piattaforma Gestione Deleghe (PGD), Identity Provider (IdP) e Service Provider (SP) i dati relativi ai soggetti delegante e delegato, trasmessi all'interno dei flussi di autenticazione (SAML e OIDC), DEVONO essere limitati a quanto richiesto dal SP in fase di autenticazione, secondo le capacità degli specifici protocolli di autenticazione e con gli stessi attributi sia per il delegante che per il delegato.

Protocollo di scambio tra SP e IdP

Per i dettagli implementativi e gli aspetti normativi del protocollo descritto per i flussi “Richiesta di accesso al servizio online dei SP” e “Accesso al servizio online del SP” del precedente diagramma, si rimanda alle specifiche tecniche di autenticazione Regole Tecniche CIE eID SAML, Regole Tecniche SPID SAML e SPID/CIE OpenID Connect Regole tecniche.

Viene comunque di seguito riportato lo schema delle chiamate necessarie ad implementare i due flussi per dare evidenza delle necessarie differenze introdotte allo scopo di integrare la PGD nel sistema di autenticazione.

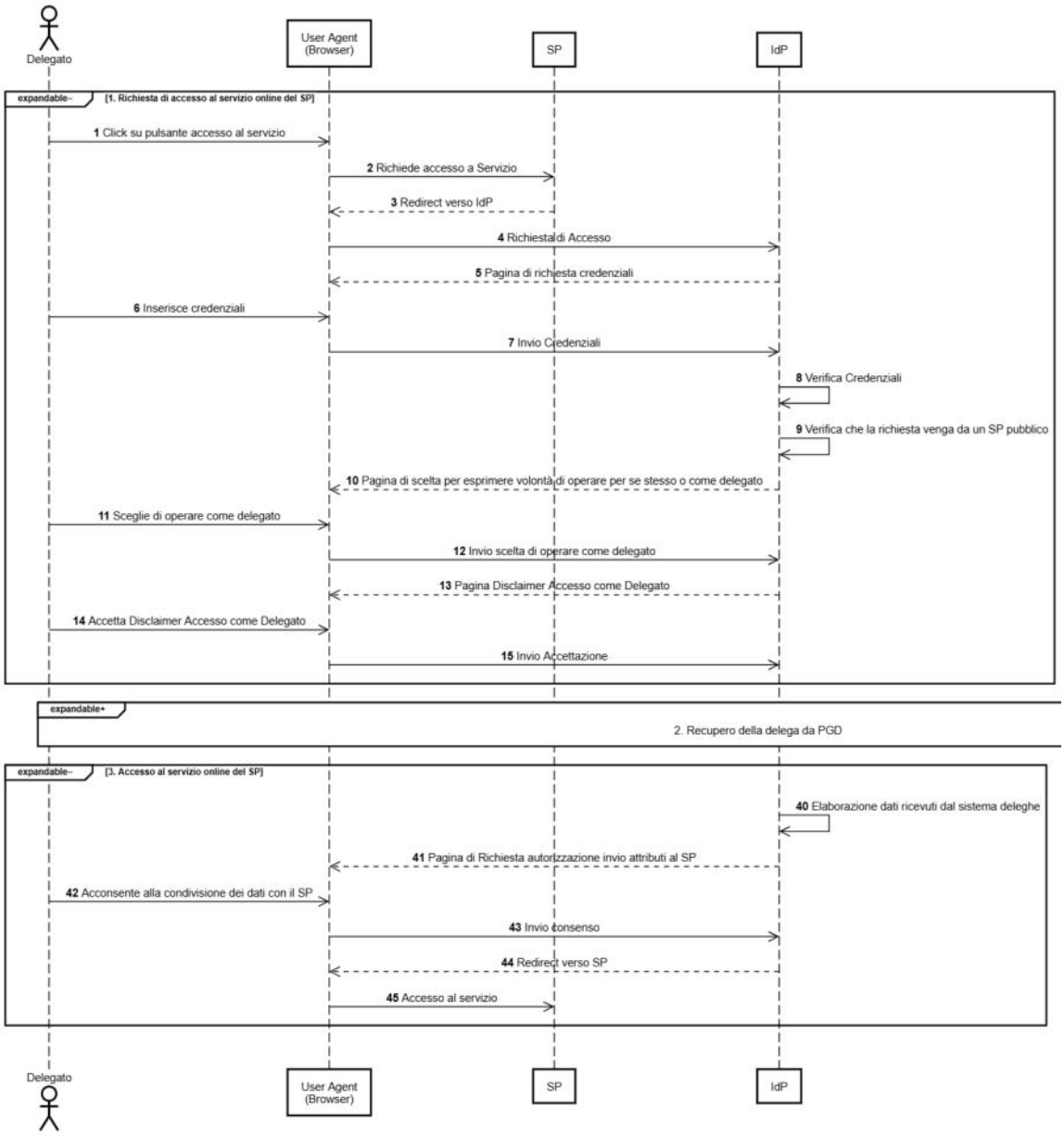


Figura 3 Protocollo di scambio tra SP e IdP

Alla ricezione di una richiesta di accesso, l'IdP DEVE verificare che il SP che ha generato la richiesta abbia aderito alla PGD e che sia parte della Pubblica Amministrazione.
La verifica di adesione deve essere effettuata secondo quando descritto al paragrafo Gestione Abilitazione dei Service Provider.

Successivamente l'IdP DEVE verificare l'intenzione dell'utente che sta effettuando l'autenticazione come delegato e DEVE informarlo delle implicazioni legali che tale scelta comporta.

Al termine del flusso di autenticazione l'IdP DEVE inoltre raccogliere l'autorizzazione dell'utente ad inviare i dati della delega (nello specifico i dati anagrafici del delegante e del delegato) al SP che ha originato la richiesta di autenticazione.

Infine, l'accesso ai dati di delega deve disabilitare qualsiasi meccanismo di rinnovo della sessione tra IdP e SP, sia in SAML, sia in OIDC. Questo per non consentire il riutilizzo dei dati della delega senza aver richiesto una nuova autenticazione utente e senza aver richiesto le opportune verifiche di validità della delega sulla PGD.
In caso di accesso come delegato, DEVE quindi essere disabilitata la generazione e propagazione dei "refresh_token" per OIDC.
Mentre per quanto riguarda SAML DEVONO essere configurati valori fissi e brevi per il parametro "SessionNotOnOrAfter", il parametro "ForceAuthn" DEVE essere valorizzato a "true" e DEVONO essere disabilitati anche eventuali meccanismi di keep-alive lato IdP.

Questo è necessario per evitare che un'autenticazione possa essere riutilizzata per ottenere nuovi dati di delega senza richiedere una nuova autenticazione utente.

OIDC

Nel protocollo OIDC, a seguito di una richiesta di accesso ad un Relying Party (RP), viene generata una Authorization Request che una volta inviata all'IdP avvia il flusso di autenticazione utente.

Al termine del flusso di autenticazione, il RP ottiene dall'IdP (quest'ultimo anche denominato OpenID Provider) un "access_token" tramite il quale può invocare l'endpoint /userInfo per accedere ai dati dell'utente che si è autenticato.

In aggiunta ai parametri definiti nelle Regole Tecniche OIDC per SPID e CIE id, con l'introduzione della PGD, l'OpenID Provider (OP) DEVE inviare al RP i seguenti parametri:

- **is_delegate**: [OBBLIGATORIO]. Booleano. Valorizzato a true se l'utente ha effettuato l'accesso con delega e a false altrimenti.
- **delegation_info**: [CONDIZIONALE]. Stringa. Se is_delegate è valorizzato a true, DEVE contenere il payload del JWT delegation_info restituito dalla PGD.

In caso di accesso come delegato tutti gli attributi identificativi dell'utente richiesti dal RP DEVONO essere valorizzati con i dati del delegante (e non con i dati dell'utente che ha effettuato l'accesso e inserito le credenziali).
Nel contesto "CIE ID" gli attributi dell'utente sono disponibili sia nell'ID Token, sia nella UserInfo Response. Nei casi in cui ID Token e UserInfo siano equivalenti, quanto appena descritto per la UserInfo, quindi, DEVE valere anche per l'ID Token.

Segue un esempio non normativo della risposta in caso di accesso con delega:

```
{
      "name": "Mario",
      "family_name": "Rossi",
      "birth_date": YYYY-MM-DD,
```

```
      "https://attributes.spid.gov.it/fiscal_number": "MROXXXXXXXXXXXXX",
      "is_delegate": true,
      "delegation_info":"eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjNmMjMx
Yjk5LWY2ZDYtMjUxOC0wN2I5LTA4ZDA5MTNmZDI4ZCJ9.eyJpc3MiOiJodHRwczovL3BnZC5nb3Yu
aXQiLCJhdWQiOiJodHRwczovL2lkcC5leGFtcGxlLm9yZyIsInZlcnNpb24iOiIxLjAiLCJkZWxlZ
2F0ZSI6eyJuYW1lIjoiTWFyaW8iLCJmYW1pbHlfbmFtZSI6IlJvc3NpIiwiYmlydGhkYXRlIjoiMT
k2NS0xMi0xMCIsImZpc2NhbF9udW1iZXIiOiJSU1NNUkE2NVQxMEgwMjdYIn0sImRlbGVnYXRvciI
6eyJuYW1lIjoiR2l1c2VwcGUiLCJmYW1pbHlfbmFtZSI6IlZlcmRpIiwiYmlydGhkYXRlIjoiMTk3
NS0wNS0yMCIsImZpc2NhbF9udW1iZXIiOiJWUkRHUFA3NUUyMEYyMDVBIn0sInR5cGUiOiJwYXJlb
nRhbF9yZXNwb25zaWJpbGl0eSIsImlhdCI6MTczMTg1MzYzNCwibmJmIjoxNzMxODUzNjM0LCJleH
AiOjE3MzE4NTcyMzR9.signature"
}
```


SAML

Nel protocollo SAML, a seguito di una richiesta di accesso ad un SP viene generata una AuthnRequest che una volta inviata all'IdP avvia il flusso di autenticazione utente.

Al termine del flusso di autenticazione il SP ottiene una SAML Response dall'IdP contenente una "<saml:Assertion>" con i dati dell'utente autenticato.

.

In aggiunta ai parametri definiti nelle Regole Tecniche SAML per SPID e CIE eID, con l'introduzione della PGD, l'IdP DEVE inviare al SP i seguenti parametri:

- **isDelegate**: [OBBLIGATORIO]. Valorizzato a true se l'utente ha effettuato l'accesso con delega e false altrimenti.
- **delegationInfo**: [CONDIZIONALE]. Oggetto. Se is_delegate è valorizzato a true, DEVE contenere i seguenti parametri estratti dal delegation_info restituito dalla PGD:
    - **jwt**: [OBBLIGATORIO]. Stringa. DEVE contenere il JWT così come ottenuto da PGD durante il flusso di richiesta della delega per consentire ai SP di effettuare la verifica di autenticità delle informazioni di delega;
    - **delegate**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegato;
        - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegato;
        - **familyName**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegato;
        - **dateOfBirth**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegato nel formato ISO 8601 (YYYY-MM-DD).
        - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo email del delegante se disponibile;
        - **fiscalNumber**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegato.
    - **delegator**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegante;
        - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegante;
        - **familyName**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegante;
        - **dateOfBirth**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegante nel formato ISO 8601 (YYYY-MM-DD).
        - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo email del delegante se disponibile;

        - **fiscalNumber**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegante.
    - **type**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo del tipo di delega conferita al delegato *(vedere tab. 1)*;
    - **iat**: [OBBLIGATORIO]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di creazione della delega. Il tipo XML associato è xs:dateTime;
    - **nbf**: [OPZIONALE]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di creazione della delega. Il tipo XML associato è xs:dateTime;
    - **exp**: [OBBLIGATORIO]. Stringa/DataOra. DEVE contenere un timestamp formattato come ISO 8601 (es. YYYY-MM-DDThh:mm:ssZ) che indica la data di creazione della delega. Il tipo XML associato è xs:dateTime

In caso di accesso come delegato, tutti gli attributi identificativi dell'utente richiesti dal SP DEVONO essere valorizzati con i dati del delegante (e non con i dati dell'utente che ha effettuato l'accesso e inserito le credenziali).

Segue un esempio non normativo di Attribute Statement in caso di accesso con delega.

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                          xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

  <!-- Attributi utente autenticato (delegato) -->
  <saml2:Attribute FriendlyName="Nome" Name="name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Mario</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome" Name="familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Rossi</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data di Nascita" Name="dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1965-12-
10</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Codice Fiscale" Name="fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">TINIT-
RSSMRA65T10H027X</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Flag: utente accede come delegato -->
  <saml2:Attribute FriendlyName="Accede come Delegato" Name="isDelegate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
```

```
    <saml2:AttributeValue xsi:type="xs:boolean">true</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- ======================================== -->
  <!-- DelegationInfo - Attributi destrutturati  -->
  <!-- ======================================== -->

  <saml2:Attribute FriendlyName="Versione Delega"
Name="delegationInfo.version"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1.0</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Informazioni Delegato -->
  <saml2:Attribute FriendlyName="Nome Delegato"
Name="delegationInfo.delegate.name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Mario</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome Delegato"
Name="delegationInfo.delegate.familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Rossi</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data di Nascita Delegato"
Name="delegationInfo.delegate.dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1965-12-
10</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Codice Fiscale Delegato"
Name="delegationInfo.delegate.fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">RSSMRA65T10H027X</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Informazioni Delegante -->
  <saml2:Attribute FriendlyName="Nome Delegante"
Name="delegationInfo.delegator.name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">Giuseppe</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Cognome Delegante"
Name="delegationInfo.delegator.familyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">Verdi</saml2:AttributeValue>
  </saml2:Attribute>
```

```
  <saml2:Attribute FriendlyName="Data di Nascita Delegante"
Name="delegationInfo.delegator.dateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xsi:type="xs:string">1975-05-
20</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Codice Fiscale Delegante"
Name="delegationInfo.delegator.fiscalNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">VRDGPP75E20F205A</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- Metadata Delega -->
  <saml2:Attribute FriendlyName="Tipo di Delega" Name="delegationInfo.type"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue
xsi:type="xs:string">parental_authority_holder</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data Creazione Delega"
Name="delegationInfo.iat" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T14:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data Inizio Validità Delega"
Name="delegationInfo.nbf" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T14:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

  <saml2:Attribute FriendlyName="Data Fine Validità Delega"
Name="delegationInfo.exp" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
    <saml2:AttributeValue xsi:type="xs:dateTime">2024-11-
17T15:33:54Z</saml2:AttributeValue>
  </saml2:Attribute>

  <!-- ======================================== -->
  <!-- JWT completo firmato da PGD              -->
  <!-- ======================================== -->

  <saml2:Attribute FriendlyName="Delegation Info JWT"
Name="delegationInfo.jwt" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
    <saml2:AttributeValue
xsi:type="xs:string">eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjNmMjMxYjk5
LWY2ZDYtMjUxOC0wN2I5LTA4ZDA5MTNmZDI4ZCJ9.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQi
```

```
LCJhdWQiOiJodHRwczovL2lkcC5leGFtcGxlLm9yZyIsInZlcnNpb24iOiIxLjAiLCJkZWxlZ2F0Z
SI6eyJuYW1lIjoiTWFyaW8iLCJmYW1pbHlfbmFtZSI6IlJvc3NpIiwiYmlydGhkYXRlIjoiMTk2NS
0xMi0xMCIsImZpc2NhbF9udW1iZXIiOiJSU1NNUkE2NVQxMEgwMjdYIn0sImRlbGVnYXRvciI6eyJ
uYW1lIjoiR2l1c2VwcGUiLCJmYW1pbHlfbmFtZSI6IlZlcmRpIiwiYmlydGhkYXRlIjoiMTk3NS0w
NS0yMCIsImZpc2NhbF9udW1iZXIiOiJWUkRHUFA3NUUyMEYyMDVBIn0sInR5cGUiOiJwYXJlbnRhb
F9yZXNwb25zaWJpbGl0eSIsImlhdCI6MTczMTg1MzYzNCwibmJmIjoxNzMxODUzNjM0LCJleHAiOj
E3MzE4NTcyMzR9.signature</saml2:AttributeValue>
  </saml2:Attribute>

</saml2:AttributeStatement>
```


Protocollo di scambio tra IdP e PGD

In questa sezione viene descritto il flusso tecnico di interazione e scambio dati tra l'IdP e la PGD. Tale protocollo si basa sul framework OAuth 2.0 e, in particolare, prevede l'utilizzo delle seguenti specifiche tecniche di riferimento e standard:

- The OAuth 2.0 Authorization Framework [RFC6749];
- Proof Key for Code Exchange (PKCE) [RFC7636];
- Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC7521];
- OAuth 2.0 Pushed Authorization Requests (PAR) [RFC9126];
- OAuth 2.0 Rich Authorization Requests (RAR) [RFC9396];
- The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR) [RFC9101]
- OAuth 2.0 Authorization Server Issuer Identification [RFC9207]
- OAuth 2.0 Demonstrating Proof of Possession (DPoP) [RFC9449].

Per garantire l'integrità e confidenzialità della comunicazione tra PGD e IdP è RICHIESTO l'utilizzo di chiavi di firma e cifratura in accordo alla Sezione “Algoritmi Supportati” presenti in questo documento.
Le modalità di scambio delle chiavi DEVE essere fatta tramite processi out-of-band che non vengono definiti all'interno di questa specifica.
Per garantire l'integrità e confidenzialità della comunicazione tra PGD e IdP si RACCOMANDA in ogni caso l'utilizzo di chiavi di firma e cifratura ad hoc, non già utilizzate per altre finalità.
In tutte le comunicazioni tra le parti, DEVE essere utilizzato il protocollo TLS nella versione 1.2 o superiore. L'utilizzo di versioni precedenti del protocollo TLS o del protocollo SSL è espressamente vietato.

Il diagramma di seguito riportato descrive il dettaglio del protocollo di scambio.

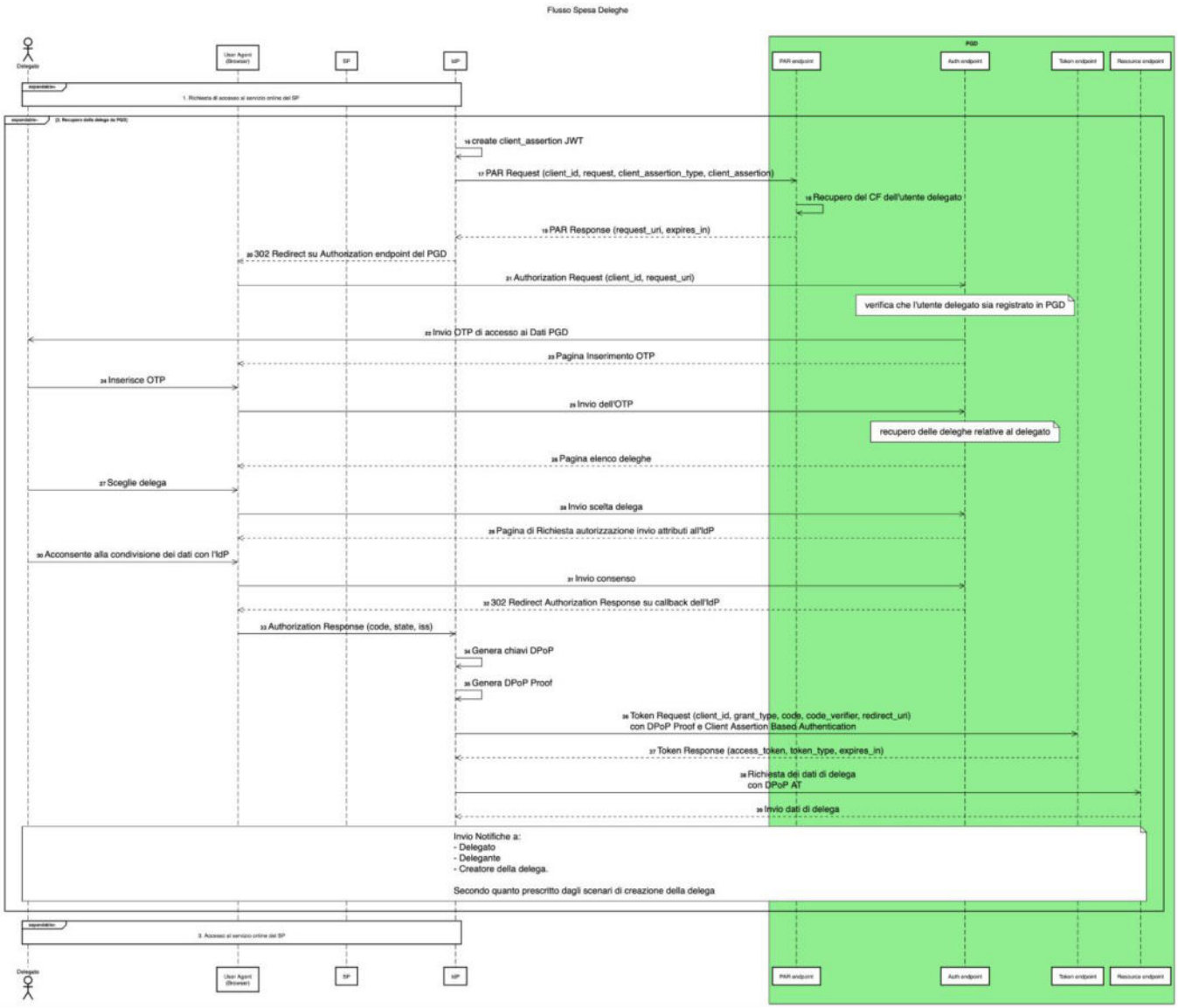


Figura 4 Protocollo di scambio tra

Nel diagramma sopra riportato, gli step da 1 a 16 descrivono la fase di richiesta di accesso ai servizi online del SP durante il protocollo di scambio tra SP e IdP (vedi sezione “Protocollo di scambio tra SP e IdP”.

Segue la descrizione dei passi, a partire dallo step 16, che compongono questa porzione del flusso.

Step 16: L'IdP crea un JWT “**$clientAssertion**” (contenente informazioni come il Codice Fiscale del delegato e altri dettagli volti a garantire l'autenticità della richiesta di accesso alla PGD da parte dell’IdP).

Step 17: L'IdP invia una richiesta al PAR endpoint della PGD con le informazioni necessarie.

A seguito della ricezione della richiesta di PAR da parte dell'IdP, la PGD DEVE verificare:

- la validità e le firme della "**$clientAssertion**" e del "**$responseObjec**t" inviati dall'IdP;
- la corrispondenza tra i parametri nel JWT e quelli nella richiesta HTTP il binding tra Request Object e client assertion attraverso il "client_id".

La PGD DEVE inoltre verificare l'unicità del parametro "**jti**", la validità temporale della richiesta e la conformità dei campi "**iss**", "**sub**" e "**aud**".
La PGD DEVE estrarre e verificare il contenuto di "**authorization_details**".
La PGD DEVE verificare che il CF contenuto dal parametro "**identifier**" corrisponda ad un CF precedentemente registrato in PGD.
La PGD DEVE verificare i parametri **scope** e **claims**, per restituire all'IdP i soli dati del delegante e delegato richiesti e disponibili. Qualora i campi siano assenti la PGD DEVE restituire il minimum dataset eIDAS.
In caso di fallimento della PAR, la PGD DEVE rispondere con un errore. L'IdP DEVE presentare all'utente un'apposita schermata di errore che lo informa dell'esito della richiesta. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 18: la PGD recupera il Codice Fiscale del delegato.

Step 19: la PGD risponde alla PAR con un "**request_uri**" valido per un tempo ridotto che consente di effettuare una Authentication Request.

Step 20: L'IdP reindirizza il browser all'endpoint di autorizzazione della PGD.

Step 21: Il browser invia la richiesta di autorizzazione al PGD (inclusi **client_id** e **request_uri**).

Alla ricezione della richiesta la PGD DEVE verificare la validità della "**request_uri**" della richiesta e recupera i dati relativi al Codice Fiscale del delegato precedentemente salvati in sessione.
Successivamente la PGD verifica che l'utente (Delegato) sia registrato nel sistema.

In caso di fallimento della PAR, la PGD DEVE rispondere con un errore. L'IdP DEVE presentare all'utente un'apposita schermata di errore che lo informa dell'esito della richiesta. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 22: La PGD invia un OTP al Delegato per consentirgli l'accesso ai dati delle deleghe.

L'OTP DEVE essere generato randomicamente, alfanumerico, lungo almeno sei caratteri ed essere inviato sulla e-mail certificata del Delegato raccolta durante il processo di creazione o accettazione della delega. Tale OTP DEVE avere durata non superiore a due minuti ed essere utilizzabile per un solo tentativo di accesso. Nell'ambito della stessa sessione di autenticazione e alla scadenza di un OTP, la PGD DEVE consentire all'utente di effettuare una nuova richiesta di OTP. Inoltre, PGD DEVE implementare meccanismi di rate limiting per codice fiscale e indirizzo IP con lockout temporaneo dopo un numero massimo di tentativi (es. lockout di 1 ora dopo 10 tentativi falliti) e registrare l'evento per analisi di sicurezza. La PGD DEVE inoltre implementare logging e monitoring per rilevare pattern di attacco (es. richieste massive, tentativi distribuiti).

La mail contenente l'OTP DEVE mostrare l'informazione relativa al SP.

Step 23: La PGD mostra la pagina di inserimento dell'OTP.

La schermata di inserimento DEVE mostrare l'informazione relativa al nome del SP.

Step 24: Il delegato inserisce l'OTP.

Step 25: Il browser invia l'OTP alla PGD che ne verifica la validità.

La PGD DEVE verificare la correttezza dell'OTP e recupera le deleghe a lui associate (se presenti) e ne restituisce l'elenco al browser.

In caso di errato inserimento dell'OTP da parte dell'utente, la PGD DEVE mostrare una pagina di errore e DEVE consentire all'utente di richiedere un nuovo OTP. La PGD DEVE consentire al più due richieste di OTP nell'ambito della medesima sessione di autenticazione.

Nel caso in cui l'OTP inserito dall'utente sia correttamente validato dalla PGD, quest'ultima DEVE effettuare le verifiche di validità della delega in accordo con lo scenario di creazione della delega scelta, secondo quanto prescritto dal DCPM DELEGHE e dal relativo allegato tecnico.

In caso di fallimento dell'ultimo tentativo di inserimento dell'OTP da parte dell'utente, o delle verifiche di validità della delega, la PGD DEVE restituire una risposta di errore all'IdP mostrando all'utente una pagina di errore. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 26: La PGD mostra la pagina di scelta delle deleghe.

Step 27: Il Delegato sceglie una delega specifica sulla PGD.

La PGD DEVE consentire di annullare il flusso di accesso con delega in qualsiasi momento, per contemplare, ad esempio, il caso in cui l'utente non trovi nella lista delle deleghe disponibili quella che intendeva utilizzare.

Step 28: Il browser invia la scelta della delega al PGD.

Step 29: la PGD chiede all'utente (Delegato) l'autorizzazione ad inviare gli attributi all'IdP.

In caso di mancata autorizzazione, la PGD DEVE restituire una risposta di errore all'IdP mostrando all'utente una pagina di errore. L'IdP NON DEVE consentire all'utente di proseguire il flusso di autenticazione con delega e DEVE restituire un errore al SP.

Step 30: L'utente (Delegato) autorizza la condivisione dei dati.

Step 31: Il browser invia l'autorizzazione al PGD.

Step 32: la PGD reindirizza il browser all'IdP con il codice di autorizzazione.

Step 33: Il Browser effettua la richiesta di autorizzazione all'IdP.

Step 34: L'IdP genera delle chiavi asimmetriche effimere.

Step 35: L'IdP genera una prova DPoP con le chiavi effimere appena create.

Step 36: L'IdP richiede un token all'endpoint **/token** della PGD inviando, con un'apposita richiesta contenente nell'HTTP Header DPoP, la prova DPoP alla PGD.

Alla ricezione della richiesta, la PGD DEVE validare la DPoP Proof:

- Verificandone la firma usando la chiave JWK nell'header;
- Validando il tipo "**dpop+jwt**";
- Verificando l'unicità del jti;
- Verificando che htm e htu corrispondano alle specifiche del **/token** endpoint;
- Verificando la validità temporale della richiesta;
- Verificando il "**code_verifier**" rispetto alla "**code_challenge**" originale;
- Verificando che il redirect_uri corrisponda a quello della richiesta originale;
- Verificando che la chiave usata per il DPoP Proof sia la stessa usata in precedenza.

La PGD DEVE, inoltre, memorizzare il thumbprint della chiave JWK e creare il Binding del thumbprint con l'access token generato.

Step 37: la PGD risponde con un "**access_token**".

La PGD NON DEVE MAI includere refresh token nella risposta, onde evitare che possa essere prolungata una sessione precedente per ri-ottenere i dati di una delega.

Step 38: L'IdP richiede i dati della delega al PGD usando il token ottenuto.

Step 39: la PGD invia i dati della delega (in particolare invia i dati del minimum dataset eIDAS del delegante in chiaro).

La PGD deve inoltre mandare l'informazione relativa al nome del SP nelle e-mail di notifica di accesso ai dati delle deleghe.

Le specifiche di UX/UI non sono definite all'interno di questa specifica.

Endpoint IdP-PGD

La PGD DEVE esporre i seguenti endpoint HTTP:

Endpoint	Metodo	Descrizione	Autenticazione
/pgd/registry	GET	Recupero del registro degli SP abilitati	Nessuna (da valutare se usare MTLS con IdP)

Endpoint	Metodo	Descrizione	Autenticazione
/as/par	POST	Pushed Authorization Request	Client Assertion
/authorize	GET	Authorization Request	Nessuna (session-based)
/token	POST	Token Request	Client Assertion + DPoP
/get-delegation-data	GET	Recupero dati delega	DPoP Access Token

Tutti gli endpoint DEVONO essere esposti tramite protocollo HTTPS (TLS 1.2 o superiore).

Gli endpoint di onboarding e gestione del ciclo di vita dei SP (/pgd/sp/*) sono definiti nella sezione "Gestione Abilitazione dei Service Provider".

Endpoint del Registro

La PGD DEVE esporre un endpoint pubblico (/pgd/registry) per la distribuzione del registro degli SP abilitati.

Richiesta HTTP

La richiesta HTTP di download del Registro JWT DEVE essere inviata all'endpoint /pgd/registry usando il metodo GET, come riportato nel seguente esempio non normativo.

```
GET /pgd/registry HTTP/1.1
Host: pgd.gov.it
Accept: application/jwt
```

Risposta HTTP

A seguito di una richiesta HTTP, la PGD DEVE:

- Calcolare dinamicamente il valore max-age dell'header Cache-Control come exp - tempo_corrente
- inviare nel body dell'HTTP Response un JWT in formato compatto, firmato dalla PGD e che rappresenta il registro degli SP abilitati.

L'HTTP Response Headers DEVE contenere i seguenti parametri:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con application/jwt.
- **Cache-Control**: [OBBLIGATORIO]. DEVE contenere la direttiva max-age con valore dinamico calcolato come max-age = exp - tempo_corrente dove exp è il claim di scadenza del JWT e tempo_corrente è il timestamp UNIX al momento della generazione della risposta HTTP. Esempio: Cache-Control: max-age=86400.
- **Last-Modified**: [OBBLIGATORIO]. Stringa. Data e ora dell'ultima modifica del Registro JWT (timestamp di generazione)

Di seguito un esempio non normativo della risposta HTTP.

```
HTTP/1.1 200 OK
Content-Type: application/jwt
Cache-Control: max-age=86400
Date: Fri, 17 Jan 2026 12:00:00 GMT
Last-Modified: Fri, 17 Jan 2026 00:00:05 GMT

eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNmMjMxYjk5LWY2ZDYtNDUxOC0wN2I5L
TA4ZDA5MTNmZDI4ZCJ9.eyJpc3MiOiJodHRwczovL3BnZC5nb3YuaXQiLCJpYXQiOjE3MzQ5NjAwM
DAsImV4cCI6MTczNTA0NjQwMCwic2FtbF9lbnRpdHlfaWRzIjpbImh0dHBzOi8vc3AxLmV4YW1wbG
Uub3JnIiwiaHR0cHM6Ly9zcDMuZ292Lml0L3NlcnZpY2VzL2RlbGVnaGUiXSwib2lkY19jbGllbnR
faWRzIjpbImh0dHBzOi8vc3AyLmV4YW1wbGUuZ292Lml0Il19.MEYCIQCa1b2c3d4e5f6g7h8i9j0
k1l2m3n4o5p6q7r8s9t0u1v2wIwQHx3y4z5a6b7c8d9e0f1g2h3i4j5k6l7m8n9o0p1q2r3s4t5u6
```

Il formato del Registro JWT è definito nella sezione "Formato del Registro JWT".

La gestione degli errori DEVE seguire quanto previsto dalle specifiche OAuth 2.0.

Verifiche dell'IdP

Gli IdP che consumano questo endpoint DEVONO:

1. **Implementare refresh proattivo**: Gli IdP DEVONO implementare un meccanismo di refresh proattivo che scarica il Registro JWT dalla PGD prima della scadenza (exp), evitando latenze durante l'autenticazione degli utenti e gestendo eventuali indisponibilità temporanee della PGD. Il refresh proattivo consente di mantenere sempre in cache un registro valido.

2. **Fallback a refresh sincrono**: In caso di mancato refresh proattivo (es. primo avvio, scadenza registro, failure dello scheduler), l'IdP PUÒ effettuare un refresh sincrono durante il flusso di autenticazione, ma questo approccio NON DOVREBBE essere implementato in produzione per

evitare latenze user-facing. In caso di fallimento del refresh sincrono, l'IdP NON DEVE fornire all'utente l'opzione di accesso con delega.

3. **Verificare la firma del JWT**: Prima di utilizzare il contenuto del registro, l'IdP DEVE verificare la firma del JWT utilizzando la chiave pubblica della PGD distribuita secondo quanto specificato nella sezione "Distribuzione Chiave Pubblica PGD".

4. **Verificare la validità temporale**: L'IdP DEVE verificare che il JWT non sia scaduto controllando il claim exp.

5. **Rispettare Cache-Control**: L'IdP DEVE rispettare l'header Cache-Control fornito dalla PGD e memorizzare in cache il Registro JWT per una durata NON superiore a max-age e NON superiore alla scadenza JWT (exp).

6. **Verifica abilitazione SP**: Durante il flusso di autenticazione, l'IdP DEVE verificare la presenza dell'identificativo del SP (entityID per SAML o client_id per OIDC) nell'array appropriato (saml_entity_ids o oidc_client_ids). Solo se l'identificativo è presente e il JWT è valido, l'IdP PUÒ offrire l'opzione di autenticazione con delega

Quando la PGD revoca un SP (revoca amministrativa o offboarding), l'identificativo del SP viene rimosso dall'array saml_entity_ids o oidc_client_ids. La revoca diventa effettiva presso gli IdP entro massimo 24 ore (al prossimo refresh proattivo o sincrono). La frequenza di generazione del Registro JWT da parte della PGD PUÒ essere inferiore a 24 ore per garantire propagazione più rapida delle revoche.

Client Authentication

A garanzia della sicurezza delle comunicazioni, l'IdP DEVE autenticarsi all'Authorization Server della PGD secondo le specifiche descritte in Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC7521].

Il sistema DEVE quindi, implementare un meccanismo di autenticazione di Client Authentication che prevede la generazione di una assertion in formato JWT (**$clientAssertion**) firmata dall'IdP (il Client) e verificata dall'Authorization Server della PGD.

Tale assertion attesta l'identità del client ('IdP) e viene trasmessa come parte della richiesta HTTP. La client authentication basata su JWT DEVE essere utilizzata sia per le richieste verso il PAR endpoint che per quelle dirette al Token endpoint della PGD e nei seguenti paragrafi ne viene presentata la specifica.

Il Client Assertion JWT **($clientAssertion**) DEVE contenere i seguenti campi:

Parametri dell'header:

- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **x5c**. Stringa. DEVE contenere l'identificativo univoco della chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT;

- **x5c**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **kid**. Stringa. DEVE contenere il certificato x.509 relativo alla chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. Identificativo univoco URL HTTPS dell'IdP richiedente;
- **sub**: [OBBLIGATORIO]. Stringa. Identificativo univoco URL HTTPS dell'IdP richiedente;
- **nbf**: [OBBLIGATORIO]. Intero. Timestamp Unix che indica il momento di inizio validità del token;
- **exp**: [OBBLIGATORIO]. Intero. Timestamp Unix che indica il momento di scadenza del token;
- **aud**: [OBBLIGATORIO]. Stringa. URL dell'endpoint Authorization della PGD;
- **jti**: [OBBLIGATORIO]. Stringa. Identificativo univoco del JWT in formato UUID v4 per prevenire replay attacks;
- **session_id**: [OPZIONALE]. Stringa. Identificativo di sessione.

Di seguito, un esempio non normativo di "$**clientAssertion**":

```
{
      "typ": "JWT",
      "alg": "ES256",
      "kid": "cde6a4c1-3032-4a64-be15-18973dc3ad9e"
}
.
{
      "iss": "https://IdP.example.org",
      "sub": "https://IdP.example.org",
      "nbf": 1300815780,
      "exp": 1300819380,
      "aud": "https://pgd.example.org/auth",
      "jti": "e958c478-0b58-4dfa-a89b-87b317acc5f1"
}
```

PAR Endpoint

Il PAR endpoint DEVE:

- essere protetto dal meccanismo di client authentication come definito nella Sezione "Client Authentication";
- utilizzare il parametro **request** come definito in JAR [RFC9101] per inviare il Request JWT Object all'Authorization Server di PGD;
- utilizzare il parametro **authorization_details** come definito in RAR [RFC9396] per veicolare l'identificativo dell'utente delegato per il quale si richiedono le informazioni di delega.

PAR Request

La richiesta PAR (Pushed Authentication Request) DEVE usare il metodo POST.

La HTTP Request DEVE contenere il seguente HTTP Header:

- **Content-type**: [OBBLIGATORIO]. Stringa. Valorizzato con **application/x-www-form-urlencoded**.

La HTTP Request DEVE contenere i seguenti query parameters:

- **client_id**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'IdP registrato presso la PGD in formato HTTPS URL;
- **state**: [OBBLIGATORIO]. Stringa casuale di lunghezza minima 32 caratteri che DEVE essere inclusa nelle successive risposte per prevenire attacchi di tipo CSRF;
- **request**: [OBBLIGATORIO]. Stringa. DEVE contenere un JWT **$requestObject**;
- **client_assertion_type**: [OBBLIGATORIO]. DEVE essere valorizzato con la stringa **urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer**;
- **client_assertion**: [OBBLIGATORIO]. DEVE contenere un JWT firmato dall'IdP contenente le informazioni di autenticazione (**$clientAssertion**).

Di seguito, un esempio non normativo della richiesta:

```
POST /as/par HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded

&client_id=https%3A%2F%2FIdP.example.org
&state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
&request=$requestObject
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
&client_assertion=$clientAssertion
```

La PAR Request DEVE contenere un JWT firmato ($requestObject) con i seguenti campi:

Parametri dell'header:

- **typ:** [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **"oauth-authz-req+jwt"**;
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **x5c**. Stringa. DEVE contenere l'identificativo univoco della chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT;
- **x5c**: [CONDIZIONALE]. OBBLIGATORIO se non è presente il parametro **kid**. Stringa. DEVE contenere il certificato x.509 relativo alla chiave pubblica dell'IdP utilizzata per la verifica della firma del JWT.

Parametri del payload:

- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL dell'endpoint PAR della PGD;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **response_type**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **code**;
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP registrato presso la PGD;

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL HTTPS dell'Identity Provider che ha emesso il token;
- **state**: [OBBLIGATORIO]. Stringa. DEVE contenere un valore opaco per mantenere lo stato tra la richiesta e il callback;
- **scope**: [OPZIONALE]. Stringa. DEVE contenere lo scope specificato nella richiesta di autenticazione OIDC originale ricevuta dall'IdP.
- **claims**: [OPZIONALE]. JSON Object. DEVE contenere i claims specificati nella richiesta di autenticazione originale ricevuta dall'IdP. Per OIDC DEVE contenere i parametri specificati in claims, per SAML DEVE contenere l'elenco dei claim specifici nell'attributo RequestedAttribute dei metadati del SP.
- **code_challenge**: [OBBLIGATORIO]. Stringa. DEVE contenere il challenge PKCE codificato in BASE64URL;
- **code_challenge_method**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **S256**. L'IdP DEVE quindi supportare lo specifico algoritmo;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. L'Array DEVE contenere almeno un oggetto JSON contenente i seguenti parametri:
    - **type**: [OBBLIGATORIO]. Stringa. Il parametro DEVE essere valorizzato con la stringa **delegation_record**;
    - **identifier**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'utente delegato valorizzato con il codice fiscale dell'utente;
    - **service_name**: [OBBLIGATORIO]. Stringa. Nome del Service Provider per il quale l'utente ha richiesto l'accesso ai servizi. La PGD DEVE garantire che l'utente che interagisce con la PGD (ad esempio nell'inserimento dell'OTP o nella e-mail di notifica) sia sempre a conoscenza del SP che ottiene le informazioni rilasciate dalla PGD.
    - **locations**: [OBBLIGATORIO]. Array di stringhe. l'Array DEVE contenere almeno una stringa valorizzata con il Resource endpoint di PGD;
- **redirect_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL a cui la PGD DEVE reindirizzare dopo il completamento del flusso.

Segue un esempio non normativo del $**requestObject**:

```
{
      "typ": "oauth-authz-req+jwt",
      "alg": "ES256",
      "kid": "cde6a4c1-3032-4a64-be15-18973dc3ad9e"
}
.
{
      "jti": "f8555ceb-c65c-4025-9378-b6672b6149af",
      "aud": "https://pgd.esempio.org/par",
      "iat": 1715842560,
      "exp": 1715842860,
      "response_type": "code",
      "client_id": "https://IdP.example.org",
      "iss": "https://IdP.example.org",
      "state": "fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd",
      "code_challenge": "E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-cM",
      "code_challenge_method": "S256",
      "redirect_uri": "https://client.example.com/cb",
```

```
      "authorization_details": [
            {
                  "type": "delegation_record",
                  "identifier": "MROXXXXXXXXXXXXX",
                  "service_name": "Service Provider 1",
                  "locations": [ "https://pgd.example.org/" ]
            }
      ]
}
```

PAR Response

A seguito della verifica di correttezza della Request effettuata dall'IdP, il PAR endpoint DEVE inviare all'IdP una HTTP Response con HTTP Response Code valorizzato a 201 Created.

La HTTP Response DEVE contenere i seguenti HTTP Headers:

- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con **no-cache, no-store** per evitare che le informazioni contenute vengano mantenute in cache;
- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con **application/json**.

Parametri nel body:

- **request_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere un identificativo univoco che fa riferimento alla richiesta di autorizzazione memorizzata. Il valore DEVE essere **urn:ietf:params:oauth:request_uri:<reference-value>**. Il valore di **reference-value** DEVE essere generato in modo random e non predicibile secondo quanto prescritto in Sezione 10.10 di RFC6749;
- **expires_in**: [OBBLIGATORIO]. Intero. DEVE indicare il tempo di validità in secondi della **request_uri** restituita.

Si riporta, di seguito, un esempio non normativo della risposta:

```
HTTP/1.1 201 Created
Cache-Control: no-cache, no-store
Content-Type: application/json

{
      "request_uri":  "urn:ietf:params:oauth:request_uri:bwc4JK-ESC0w8acc191e-
Y1LTC2",
      "expires_in": 60
}
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Authorization Endpoint

Authorization Request

A seguito dell'ottenimento della risposta all'endpoint PAR l'IdP utilizza l'OAuth 2.0 Authorization endpoint della PGD per inviare una Authorization Request. Questa DEVE includere come query parameters il **client_id** e la **request_uri** ottenuta dalla risposta del PAR endpoint.
La richiesta di Authorize DEVE usare il metodo GET.

La HTTP Request DEVE contenere i seguenti query parameters:

- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP registrato presso la PGD in formato URL HTTPS;
- **request_uri**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco ricevuto nella risposta del PAR endpoint.

Di seguito, un esempio non normativo della richiesta:

```
GET
/authorize?client_id=https%3A%2F%2FIdP.example.org&request_uri=urn%3Aietf%3Ap
arams%3Aoauth%3Arequest_uri%3Abwc4JK-ESC0w8acc191e-Y1LTC2    HTTP/1.1    Host:
pgd.esempio.org
```

Authorization Response

L'Authorization Server DEVE reindirizzare lo User-Agent all'URL specificato nel parametro **redirect_uri** della richiesta originale e aggiungere i seguenti parametri in URLencoded format:

- **code**: [OBBLIGATORIO]. Stringa. DEVE contenere l'authorization code generato dall'Authorization Server;
- **state**: [OBBLIGATORIO]. Stringa. DEVE contenere il valore esatto dello state ricevuto nella PAR Request;
- **iss**: [OBBLIGATORIO]. Stringa. Il valore DEVE contenere l'identificativo univoco della PGD e DEVE essere una stringa in formato HTTPS URL. L'utilizzo di questo parametro è richiesto per mitigare attacchi di tipi mix-up, come descritto in RFC9207.

Segue un esempio non normativo della risposta:

```
HTTP/1.1      302      Found      Location:      https://client.example.org/cb?
code=SplxlOBeZQQYbYS6WxSbIA            &state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
&iss=https%3A%2F%2Fpgd.example.org
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Token Endpoint

Il Token endpoint DEVE essere protetto dal meccanismo di client authentication come definito nella Sezione “Client Authentication”.
Il Token endpoint DEVE, inoltre, supportare l’utilizzo di Access Token DPoP, secondo quanto definito in RFC9449 e NON DEVE rilasciare Access Token di tipo diversi da DPoP Access Token.

DPoP Proof

La DPoP Proof DEVE essere generata dall’IdP e inviata nell’header della Token Request in fase di ottenimento del DPoP Access Token e della Resource Request per la richiesta e l’ottenimento della delega dell’utente.

Nella Token Request l’IdP DEVE generare la DPoP proof come definito di seguito.

Parametri dell'header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **dpop+jwt**;
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **jwk**: [OBBLIGATORIO]. Oggetto. DEVE contenere la chiave pubblica in formato JWK in accordo a quanto previsto in RFC7517 e RFC7518.

Parametri del payload:

- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **htm**: [OBBLIGATORIO]. Stringa. DEVE contenere il metodo HTTP della richiesta;
- **htu**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL completo dell'endpoint;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token.

Di seguito, un esempio non normativo della DPoP proof:

```
{
      "typ": "dpop+jwt",
      "alg": "ES256",
      "jwk":
      {
            "kty": "EC",
            "x": "l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
            "y": "9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA",
            "crv": "P-256"
      }
}
.
{
      "jti": "f6ec98f5-d78a-4fc8-8e9d-9346166a4d3e",
      "htm": "POST",
      "htu": "https://pgd.example.org/token",
      "iat":1562262616
}
```

Nell'utilizzo del DPoP Access Token, ovvero in fase di accesso al Resource endpoint, in aggiunta ai parametri sopra riportati, l'IdP DEVE aggiungere il seguente parametro alla DPoP Proof:

- **ath**: [OBBLIGATORIO]. Stringa. DEVE contenere l'hash SHA256 dell'**access_token** ottenuto dalla PGD.

Token Request

La richiesta del token DEVE essere chiamata tramite metodo HTTP POST e contenere i seguenti HTTP header:

- **Host**: [OBBLIGATORIO]. DEVE contenere l'hostname del server;
- **DPoP**: [OBBLIGATORIO]. DEVE contenere il DPoP Proof JWT;
- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con **application/x-www-form-urlencoded.**

e parametri nel body:

- **grant_type**: [OBBLIGATORIO]. DEVE essere valorizzato con **authorization_code**;
- **code**: [OBBLIGATORIO]. DEVE contenere il codice di autorizzazione ricevuto;
- **code_verifier**: [OBBLIGATORIO]. DEVE contenere il **code_verifier** originale;
- **redirect_uri**: [OBBLIGATORIO]. DEVE corrispondere alla redirect_uri originale;
- **client_assertion_type**: [OBBLIGATORIO]. DEVE essere valorizzato con **urn:ietf:params:oauth:client-assertion-type:jwt-bearer**;
- **client_assertion**: [OBBLIGATORIO]. DEVE contenere il JWT di autenticazione del client.

Di seguito, un esempio non normativo della richiesta:

```
POST /token HTTP/1.1
Host: server.example.com
DPoP: Bearer eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrIjp7Imt0eSI6Ik\
VDIiwieCI6Imw4dEZyaHgtMzR0VjNoUklDUkRZOXpDa0RscEJoRjQyVVFVZldWQVdCR\
nMiLCJ5IjoiOVZFNGpmX09rX282NHpiVFRsY3VOSmFqSG10NnY5VERWclUwQ2R2R1JE\
QSIsImNydiI6IlAtMjU2In19.eyJqdGkiOiItQndDM0VTYzZhY2MybFRjIiwiaHRtIj\
oiUE9TVCIsImh0dSI6Imh0dHBzOi8vc2VydmVyLmV4YW1wbGUuY29tL3Rva2VuIiwia\
WF0IjoxNTYyMjYyNjE2fQ.2-GxA6T8lP4vfrg8v-FdWP0A0zdrj8igiMLvqRMUvwnQg\
4PtFLbdLXiOSsX0x7NVY-FNyJK70nfbV37xRZT3Lg
Content-Type: application/x-www-form-urlencoded

{
      "grant_type": "authorization_code",
      "code": code,
      "code_verifier": dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk,
      "redirect_uri": https://client.example.org/cb,
      "client_assertion_type":        "urn:ietf:params:oauth:client-assertion-
      type:jwt-bearer",
      "client_assertion": $clientAssertion
}
```

Token Response

In caso le verifiche effettuate sulla Token Request abbiano tutte successo, la PGD DEVE rispondere con un HTTP code 200 ed i seguenti HTTP header:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con **application/json;charset=UTF-8**;
- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con **no-store** per evitare che le informazioni contenute vengano mantenute in cache;
- **Pragma**: [OBBLIGATORIO]. DEVE essere valorizzato con **no-cache** per evitare che le informazioni contenute vengano mantenute in cache.

Il body della risposta DEVE contenere i campi:

- **access_token**: [OBBLIGATORIO]. Stringa. DEVE contenere il JWT;
- **token_type**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **DPoP**;
- **expires_in**: [OBBLIGATORIO]. Intero. DEVE indicare la durata del token in secondi;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. L'Array DEVE contenere almeno un oggetto JSON contenente i seguenti parametri:
    - **type**: [OBBLIGATORIO]. Stringa. Il parametro DEVE essere valorizzato con la stringa **delegation_record**;
    - **identifier**: [OBBLIGATORIO]. Stringa. Identificativo univoco dell'utente delegato valorizzato con il codice fiscale dell'utente;
    - **service_name**: [OBBLIGATORIO]. Stringa. Nome del Service Provider per il quale l'utente ha richiesto l'accesso ai servizi. La PGD DEVE garantire che l'utente che interagisce con la PGD (ad esempio, nell'inserimento dell'OTP o nella e-mail di notifica) sia sempre a conoscenza del SP che ottiene le informazioni rilasciate dalla PGD.
    - **locations**: [OBBLIGATORIO]. Array di stringhe. l'Array DEVE contenere almeno una stringa valorizzata con il Resource endpoint di PGD.

Di seguito, un esempio non normativo:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
      "access_token":
"ewogICAgInR5cCI6ICJhdCtqd3QiLAogICAgImFsZyI6ICJFUzI1NiIsCiAgICAia2lkIjogIjYw
MmZiYzNiLWExMTctNGE0NS1hNWQyLWM0YjhlZGRkMDQ4MiIKfS4KewogICAgImlzcyI6ICJodHRwc
zovL3BnZC5leGFtcGxlLm9yZyIsCiAgICAic3ViIjogImQ0ZTBiYjM4N2FhMjU1NmZmMzA2OTI1Zm
RmYjlhNzY1IiwKICAgICJhdWQiOiAiaHR0cHM6Ly9wZ2QuZXhhbXBsZS5vcmciLAogICAgImlhdCI
6IDE3MTU4NDI1NjAsCiAgICAiZXhwIjogMTc3ODkxNDU2MCwKICAgICJqdGkiOiAiZjk2NTVjZWIt
YzY1Yy00MDI1LTkzNzgtYjY2NzJiNjE0OWJnIiwKICAgICJjbGllbnRfaWQiOiAiaHR0cHM6Ly9pZ
HAuZXhhbXBsZS5vcmciLAogICAgImNuZiI6IHsKICAgICAgImprdCI6ICI5NTE1NzRhZWUxYmI3OT
A3YWUxZWMzMTA5ZGIyYjIyNSIKICAgIH0KfQo=",
      "token_type": "DPoP",
```

```
	"expires_in": 3600,
	"authorization_details": [
		{
			"type": "delegation_record",
			"identifier": "MROXXXXXXXXXXXXX",
			"service_name": "Service Provider 1",
			"locations": [ "https://pgd.example.org/" ]
		}
	]
}
```

Access Token

L'access_token DEVE essere un JWT con:

Parametri dell'header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **at+jwt**;
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave del PGD utilizzata per la verifica della firma del JWT. Il valore DEVE essere in formato UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della PGD in formato HTTPS URL;
- **sub**: [OBBLIGATORIO]. Stringa. DEVE contenere un identificativo univoco pairwise opaco dell'utente;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della PGD in formato HTTPS URL;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL dell'IdP;
- **cnf**: [OBBLIGATORIO]. Oggetto. DEVE contenere:
  - **jkt**: [OBBLIGATORIO]. Stringa. DEVE contenere l'hash della chiave pubblica JWK del DPoP;
- **authorization_details**: [OBBLIGATORIO]. JSON Array. Il parametro DEVE essere valorizzato come riportato nella Token Response.

Di seguito, un esempio non normativo:

```
{
	"typ": "at+jwt",
	"alg": "ES256",
```

```
      "kid": "602fbc3b-a117-4a45-a5d2-c4b8eddd0482"
}
.
{
      "iss": "https://pgd.example.org",
      "sub": "d4e0bb387aa2556ff306925fdfb9a765",
      "aud": "https://pgd.example.org",
      "iat": 1715842560,
      "exp": 1715843160,
      "jti": "f9655ceb-c65c-4025-9378-b6672b6149bg",
      "client_id": "https://idp.example.org",
      "cnf":
      {
            "jkt": "951574aee1bb7907ae1ec3109db2b225"
      },
      "authorization_details": [
            {
                  "type": "delegation_record",
                  "identifier": "MROXXXXXXXXXXXX",
                  "service_name": "Service Provider 1",
                  "locations": [ "https://pgd.example.org/" ]
            }
      ]
}
```


Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Get Delegation Data Endpoint

Get Delegation Data Request

La richiesta delle informazioni sulla delega DEVE essere effettuata all'endpoint **/get-delegation-data** con metodo HTTP GET ed i seguenti header HTTP:

- **Authorization**: [OBBLIGATORIO]. DEVE contenere il DPoP Access Token nel formato **DPoP {$accessToken}**;
- **DPoP**: [OBBLIGATORIO]. DEVE contenere il DPoP Proof JWT arricchito col campo **ath**, come descritto nella Sezione "DPoP Proof";

Il parametro **$accessToken** è un JWT che DEVE avere i seguenti campi

Parametri di header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con **at+jwt**;
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave utilizzata per la firma in UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL della PGD;
- **sub**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'utente;
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'URL della PGD;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di emissione del token;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica il momento di scadenza del token;
- **jti**: [OBBLIGATORIO]. Stringa. Contiene un identificativo univoco del JWT. DEVE essere una stringa in formato UUID v4;
- **client_id**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco dell'IdP in formato HTTPS URL;
- **cnf**: [OBBLIGATORIO]. Oggetto. DEVE contenere:
    - **jkt**: [OBBLIGATORIO]. Stringa. DEVE contenere il thumbprint della chiave DPoP.

Di seguito, un esempio non normativo della richiesta:

```
GET /get-delegation-data HTTP/1.1
Host: pgd.example.org
Authorization: DPoP
ewogICAgInR5cCI6ICJhdCtqd3QiLAogICAgImFsZyI6ICJFUzI1NiIsCiAgICAia2lkIjogIjYwM
mZiYzNiLWExMTctNGE0NS1hNWQyLWM0YjhlZGRkMDQ4MiIKfS4KewogICAgImlzcyI6ICJodHRwcz
ovL3BnZC5leGFtcGxlLm9yZyIsCiAgICAic3ViIjogImQ0ZTBiYjM4N2FhMjU1NmZmMzA2OTI1ZmR
mYjlhNzY1IiwKICAgICJhdWQiOiAiaHR0cHM6Ly9wZ2QuZXhhbXBsZS5vcmciLAogICAgImlhdCI6
IDE3MTU4NDI1NjAsCiAgICAiZXhwIjogMTc3ODkxNDU2MCwKICAgICJqdGkiOiAiZjk2NTVjZWItY
zY1Yy00MDI1LTkzNzgtYjY2NzJiNjE0OWJnIiwKICAgICJjbGllbnRfaWQiOiAiaHR0cHM6Ly9pZH
AuZXhhbXBsZS5vcmciLAogICAgImNuZiI6IHsKICAgICAgImprdCI6ICI5NTE1NzRhZWUxYmI3OTA
3YWUxZWMzMTA5ZGIyYjIyNSIKICAgIH0KfQo
DPoP:
eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrIjp7Imt0eSI6IkVDIiwieCI6Imw4d
EZyaHgtMzR0VjNoUklDUkRZOXpDa0RscEJoRjQyVVFVZldWQVdCRnMiLCJ5IjoiOVZFNGpmX09rX2
82NHpiVFRsY3VOSmFqSG10NnY5VERWclUwQ2R2R1JEQSIsImNydiI6IlAtMjU2In19.eyJqdGkiOi
ItQndDM0VTYzZhY2MybFRjIiwiaHRtIjoiUE9TVCIsImh0dSI6Imh0dHBzOi8vc2VydmVyLmV4YW1
wbGUuY29tL3Rva2VuIiwiaWF0IjoxNTYyMjYyNjE2fQ.2-GxA6T8lP4vfrg8v-
FdWP0A0zdrj8igiMLvqRMUvwnQg4PtFLbdLXiOSsX0x7NVY-FNyJK70nfbV37xRZT3Lg
```

Resource Response

In caso di esito delle verifiche positive, la PGD risponde con i dati della delega selezionata inseriti in un JWT.

La HTTP Response DEVE contenere i seguenti HTTP Header:

- **Content-Type**: [OBBLIGATORIO]. DEVE essere valorizzato con **application/json;charset=UTF-8**;
- **Cache-Control**: [OBBLIGATORIO]. DEVE essere valorizzato con **no-store** per evitare che le informazioni contenute vengano mantenute in cache;
- **Pragma**: [OBBLIGATORIO]. DEVE essere valorizzato con **no-cache** per evitare che le informazioni contenute vengano mantenute in cache.

Il body della risposta restituisce un JSON contenente nel parametro "**delegation_info**" che DEVE essere valorizzato con un JWT come definito di seguito:

Parametri di header:

- **typ**: [OBBLIGATORIO]. Stringa. DEVE essere valorizzato con "pgd-delegation-data-response+jwt ";
- **alg:** [OBBLIGATORIO]. Stringa. Vedi Algoritmi Crittografici;
- **kid**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo univoco della chiave pubblica del PGD utilizzata per la verifica della firma del JWT. Il valore DEVE essere in formato UUID v4.

Parametri del payload:

- **iss**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo della PGD che ha emesso il JWT (es. https://pgd.gov.it);
- **aud**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo dell'IdP destinatario del JWT (client_id dell'IdP che ha richiesto la risorsa);
- **version**: [OBBLIGATORIO]. Stringa. Contiene l'identificativo di versione della DelegationInfo;
- **delegate**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegato;
    - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegato;
    - **family_name**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegato;
    - **birthdate**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegato nel formato ISO 8601 (YYYY-MM-DD).
    - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo e-mail del delegato se disponibile;
    - **fiscal_number**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegato.
- **delegator**: [OBBLIGATORIO]. Oggetto. DEVE contenere i dati del delegante;
    - **name**: [OPZIONALE]. Stringa. DEVE contenere il nome del delegante;
    - **family_name**: [OPZIONALE]. Stringa. DEVE contenere il cognome del delegante;
    - **birthdate**: [OPZIONALE]. Stringa. DEVE contenere la data di nascita del delegante nel formato ISO 8601 (YYYY-MM-DD).
    - **email**: [OPZIONALE]. Stringa. DEVE contenere l'indirizzo e-mail del delegante se disponibile;
    - **fiscal_number**: [OBBLIGATORIO]. Stringa. DEVE contenere il codice fiscale del delegante.
- **delegation_type**: [OBBLIGATORIO]. Stringa. DEVE contenere l'identificativo del tipo di delega conferita al delegato *(vedere tab. 1)*;
- **iat**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica la data di creazione della delega;
- **nbf**: [OPZIONALE]. Intero. DEVE contenere un timestamp Unix che indica la data di inizio validità della delega;
- **exp**: [OBBLIGATORIO]. Intero. DEVE contenere un timestamp Unix che indica la data di fine validità della delega.

Tipologia di Delega	Attributo
Delegato generico	general_delegate
Esercente la responsabilità genitoriale	parental_authority_holder
Tutore del minore	minor_legal_guardian

Tutore dell'interdetto	incapacitated_person_guardian
Curatore	incapacitated_person_curator
Amministratore di sostegno	support_administrator
Procuratore generale	general_power_of_attorney_holder
Procuratore speciale	special_power_of_attorney_holder

Tabella 1 tipologia di delega

Di seguito, un esempio non normativo della risposta:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
      "delegation_info":"$DelegationDataResponseJWT"
}
```

Gestione Errori

La gestione degli errori va implementata in accordo con quanto previsto dalle specifiche di riferimento OAuth 2.0.

Livelli di Operatività della Delega

Scopi della Delega Generale

In fase di creazione delle deleghe, nel caso di delegato generico (**general_delegate**), il delegante PUÒ specificare il livello di operatività della delega tra le seguenti opzioni:

- **sola consultazione**: il delegato può accedere ai servizi in modalità di sola lettura/consultazione delle informazioni del delegante;
- **completo**: il delegato può operare con i medesimi privilegi del delegante, incluse operazioni di modifica, inserimento e gestione.

Per le seguenti tipologie di delega, il livello di operatività DEVE essere completo:

- Esercente la responsabilità genitoriale (parental_authority_holder)
- Tutore del minore (minor_legal_guardian)
- Tutore dell'interdetto (incapacitated_person_guardian)
- Curatore (incapacitated_person_curator)
- Amministratore di sostegno (support_administrator)
- Procuratore generale (general_power_of_attorney_holder)
- Procuratore speciale (special_power_of_attorney_holder)

Livelli di Operatività in Ambito FSE/EDS/PNT

In conformità all'art. 11, comma 12 del **"Decreto del Ministero della Salute del 7 settembre 2023"** pubblicato in **Gazzetta Ufficiale Serie Generale n. 249 del 24 ottobre 2023**, per **Fascicolo Sanitario Elettronico (FSE), Ecosistema Dati Sanitari (EDS), Piattaforma Nazionale di Telemedicina (PNT)** è previsto un oggetto informativo separato, applicabile esclusivamente alle deleghe di tipo **general_delegate**. Il delegante, in fase di creazione della delega, PUÒ specificare uno dei seguenti livelli di delega per l'accesso ai servizi in ambito FSE/EDS/PNT:

- Delega di tipo "0" (non delegato): Il delegante decide esplicitamente di escludere FSE/EDS/PNT dall'operatività del delegato.
- Delega di tipo "A": Accesso completo al FSE dell'assistito delegante con i massimi privilegi (consultazione, accesso completo ai servizi e inserimento dati)
- Delega di tipo "B": Consultazione dei dati e dei documenti relativi all'assistito.
- Delega di tipo "C": Accesso ai servizi, incluse le prestazioni dei consensi e le relative revoche, nonché oscuramenti e relative revoche.
- Delega di tipo "D": Inserimento dei dati e documenti nel taccuino personale dell'assistito.

Le deleghe di tipo **B**, **C** e **D** possono essere selezionate singolarmente o in combinazione tra loro, in base alla volontà del delegante e in conformità con l'art. 11, comma 12, lettere b), c) e d) del DM Salute del 7 settembre 2023.

Per le seguenti tipologie di delega, il livello di delega per l'ambito FSE/EDS/PNT è SEMPRE di tipo **A** (accesso completo):

- Esercente la responsabilità genitoriale (parental_authority_holder)
- Tutore del minore (minor_legal_guardian)
- Tutore dell'interdetto (incapacitated_person_guardian)
- Curatore (incapacitated_person_curator)
- Amministratore di sostegno (support_administrator)
- Procuratore generale (general_power_of_attorney_holder)
- Procuratore speciale (special_power_of_attorney_holder)

Durante la fase di onboarding il SP che fornisce servizi in ambito FSE/EDS/PNT DEVE aggiungere il seguente parametro nella richiesta di onboarding definita in sezione Endpoint di Onboarding:

- **health_delegation_type_required**: [OPZIONALE]. Booleano. Se true la PGD DEVE consentire all'utente di indicare il livello di delega desiderato per l'ambito FSE/EDS/PNT.

Integrazioni al delegation_info JWT

Alla struttura del JWT **delegation_info** definita nella sezione Get Delegation Data Endpoint si aggiungono i seguenti parametri:

- **delegation_scope**: [CONDIZIONALE]. Stringa. Se la delega è di tipo general_delegate, DEVE essere presente. Valori ammessi: "**read_only**" (solo consultazione) o "**full_access**" (completo) come definito in sezione Scopi della Delega Generale.
- **health_delegation_type**: [CONDIZIONALE]. Array di Stringhe. Se la delega è di tipo general_delegate e il SP gestisce servizi in ambito FSE/EDS/PNT, DEVE essere presente. I valori ammessi sono definiti nella sezione Livelli di Operatività in Ambito FSE/EDS/PNT. I valori "B",

"C", e "D" POSSONO essere combinati. Altre combinazioni NON DEVONO essere ammesse. Se il parametro è assente, si intende che il Service Provider non gestisce servizi in ambito FSE/EDS/PNT.

Un esempio non normativo completo del payload del delegation_info JWT è dato di seguito.

```
{
  "iss": "https://pgd.gov.it",
  "aud": "https://idp.example.org",
  "version": "1.0",
  "delegate": {
    "name": "Mario",
    "family_name": "Rossi",
    "birthdate": "1965-12-10",
    "fiscal_number": "RSSMRA65T10H027X"
  },
  "delegator": {
    "name": "Giuseppe",
    "family_name": "Verdi",
    "birthdate": "1975-05-20",
    "fiscal_number": "VRDGPP75E20F205A"
  },
  "delegation_type": "general_delegate",
  "delegation_scope": "full_access",
  "health_delegation_type": ["B", "C"],
  "iat": 1731853634,
  "nbf": 1731853634,
  "exp": 1731857234
}
```

Integrazioni in SAML e OIDC

Alle informazioni di **delegationInfo** definite nella sezione Protocollo di scambio tra SP e IdP si aggiungono i seguenti attributi:

Per SAML:

```
<saml2:Attribute FriendlyName="Ambito Operatività Delega"
  Name="delegationInfo.delegationScope"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml2:AttributeValue
xsi:type="xs:string">full_access</saml2:AttributeValue>
</saml2:Attribute>

<saml2:Attribute FriendlyName="Tipo Delega Sanitaria"
  Name="delegationInfo.healthDelegationType"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml2:AttributeValue xsi:type="xs:string">A</saml2:AttributeValue>
</saml2:Attribute>
```

Per OIDC:

I parametri **delegation_scope** e **health_delegation_type** devono essere inclusi nel payload del JWT **delegation_info** trasmesso tramite il claim dedicato.

Nota: il parametro **delegation_scope** è sempre presente nel JWT **delegation_info** per le deleghe di tipo **general_delegate**, in quanto definisce il livello di operatività generale applicabile a tutti i servizi.
Il parametro **health_delegation_type** è presente nel JWT **delegation_info** solo se il delegante ha esplicitamente configurato la delega per l'ambito FSE/EDS/PNT durante la fase di creazione della delega.
Per i SP che non gestiscono servizi FSE/EDS/PNT, il parametro **health_delegation_type** sarà assente dal JWT, garantendo la minimizzazione dei dati trasmessi.

Distribuzione Chiave Pubblica PGD

Pubblicazione

La PGD DEVE pubblicare le proprie chiavi pubbliche utilizzate per la gestione dell'abilitazione e del ciclo di vita dei SP, e del protocollo di comunicazione con gli IdP in una apposita sezione del sito istituzionale della PGD.

Il formato di pubblicazione DEVE includere per ogni chiave:

- kid (Key ID in formato UUID v4)
- Algoritmo di firma
- Chiave pubblica in formato JWK conforme a [RFC7517]
- Fingerprint SHA-256 della chiave
- Periodo di validità

Gli IdP e gli SP DEVONO configurare la chiave nei propri sistemi per consentire le verifiche previste durante i protocolli di scambio dati.
Per scopi di interoperabilità, PGD PUÒ rendere disponibili le proprie chiavi pubbliche anche tramite l'endpoint well-known "/.well-known/jwks.json", che DEVE restituire le chiavi pubbliche in formato JWKS.

Rotazione Chiavi e Notifica agli SP e agli IdP

In caso di rotazione delle chiavi di firma, la PGD DEVE:

1. Pubblicare la nuova chiave in una apposita sezione del portale istituzionale di PGD mantenendo la chiave precedente
2. Inviare notifica agli SP tramite l'indirizzo contact registrato e agli IdP tramite i contatti pubblicati nei metadata ufficiali

3. Firmare Registro JWT e Trust Mark con entrambe le chiavi (nuova e precedente) per un periodo di overlap
4. Dopo il periodo di overlap, rimuovere la chiave precedente

Il periodo di overlap DEVE essere di almeno 60 giorni.

Quando la PGD pubblica una nuova chiave, DEVE inviare una notifica all'indirizzo di contatto degli IdP e a quello registrato da ciascun SP durante l'onboarding.
La notifica DEVE contenere almeno le seguenti informazioni:

- kid della nuova chiave
- Fingerprint SHA-256
- URL di download
- Periodo di overlap (non oltre 60 giorni)
- Data scadenza chiave precedente

Gli SP e IdP DEVONO verificare il fingerprint con i riferimenti pubblicati sui canali istituzionali e di conseguenza aggiornare la propria configurazione aggiungendo la nuova chiave entro il periodo di overlap.

Gestione abilitazione dei servizi

Una volta ricevuti tutti gli attributi trasmessi dalla Piattaforma Gestione Deleghe, ricade sotto la responsabilità esclusiva del Service Provider (SP) la determinazione delle logiche di autorizzazione all'accesso ai servizi erogati, in particolare:

- Individuare eventuali servizi che non siano compatibili con l'accesso tramite delega, valutato il contesto, le finalità, le tipologie dei dati trattati e gli eventuali impatti sulla sfera giuridica del delegante e/o di terzi e, di conseguenza, non consentirne l'accesso, anche non accettando gli attributi trasmessi dalla Piattaforma.
- Eventualmente limitare funzionalmente il servizio in rete erogato (es. consentire la sola consultazione inibendo le funzionalità dispositive) sulla base degli attributi ricevuti dalla Piattaforma (tipologia di delega, perimetro di utilizzo, validità).
- Tracciare le attività di sistema mediante la definizione di una policy formale che garantisca la conservazione sicura dei log, incluse modalità di accesso per la loro consultazione, per almeno 24 mesi, documentando le procedure tecniche a tutela dell'integrità e disponibilità del dato, inclusa la registrazione obbligatoria della motivazione sottesa a qualsiasi accesso alle da parte degli operatori.

Notifiche

Il sistema DEVE implementare un meccanismo di notifica che, nei casi previsti dalla norma, informi gli utenti dell'accesso ai dati della PGD, dando evidenza del nome del SP e dell'IdP utilizzato dal delegato.
La notifica DEVE riportare i riferimenti all'informativa sul trattamento dei dati personali e la descrizione delle modalità per eventualmente revocare una delega conferita.

Logging

Il sistema PDG DEVE implementare un meccanismo di logging che registri i comportamenti anomali, gli errori e le operazioni significative in maniera tale da poter garantire la tracciabilità e la diagnostica dei vari dettagli salienti del flusso di utilizzo della delega in accordo con le misure previste da [Allegato 4].

Specifiche IdP

L'IdP DEVE pubblicare sul proprio portale istituzionale, rendendola facilmente accessibile all'utente, un'informativa sul trattamento dei dati personali redatta ai sensi dell'articolo 14 del Regolamento (UE) 2016/679 (GDPR). Tale informativa DEVE specificare le finalità e le modalità del trattamento dei dati riferiti al soggetto Delegato e Delegante nell'ambito della gestione degli accessi per conto terzi.
Nelle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi, conservate come da normativa vigente, L'IdP DEVE garantire la conservazione anche delle informazioni necessarie alle attività svolte in regime di delega.
Tali evidenze, riportando gli identificativi univoci della transazione, le date di emissione (Timestamp) e i dati relativi alla delega (is_delegate e relativi attributi), costituiscono prova tecnica opponibile per l'accertamento dell'identità del soggetto agente (Delegato) e del titolo autorizzativo (Delega).

Meccanismi di informazione tra soggetti

Al fine di garantire una corretta gestione degli incidenti di sicurezza e delle violazioni di dati personali connesse all'utilizzo della Piattaforma Gestione Deleghe (PGD), DEVONO essere previsti meccanismi di informazione tempestiva e reciproca tra il Gestore della Piattaforma, gli Identity Provider (IdP) e i Service Provider (SP).
I presenti meccanismi si applicano a:

- violazioni di dati personali relative ai trattamenti effettuati tramite la PGD;
- incidenti di sicurezza che possano incidere su disponibilità, integrità, riservatezza o autenticità dei dati e dei servizi coinvolti nei flussi PGD–IdP–SP;

fermo restando che gli obblighi di notifica verso Autorità e interessati rimangono in capo ai rispettivi titolari del trattamento.
Il Gestore, ciascun IdP e ciascun SP DEVONO:

- designare almeno un punto di contatto tecnico e, ove previsto, uno organizzativo/privacy;
- mettere a disposizione un canale di comunicazione che garantisca autenticità del mittente e integrità dei messaggi (es. PEC o canale equivalente).

Tali informazioni DEVONO essere mantenute aggiornate e rese disponibili agli altri soggetti coinvolti.

Algoritmi Supportati

Per la specifica degli algoritmi di cifratura supportati dal protocollo di rimanda alle specifiche disponibili nella Sezione Algoritmi Crittografici e Linee guida funzioni crittografiche di ACN.

Gestione degli aggiornamenti della Specifica

Queste specifiche tecniche possono essere aggiornate per motivi di sicurezza, evoluzione tecnologica o conformità a standard nazionali ed europei, nel rispetto dei principi e requisiti definiti dalla normativa di riferimento. Gli aggiornamenti DEVONO essere pubblicati sul Portale della Piattaforma di Gestione Deleghe.

Acronimi

ACRONIMO	DEFINIZIONE
ACN	Agenzia per la Cybersicurezza Nazionale
CIE	Carta di Identità Elettronica
CSRF	Cross-site Request Forgery
DPoP	Demonstrating Proof-of-Possession
IdP	Gestore delle identità digitali (Identity Provider). Sinonimo di OpenID Provider (OP), secondo il protocollo OIDC
JWKS	JSON Web Key Set
JWT	JSON Web Token
MiTM	Man in The Middle
OIDC	OpenID Connect
PAR	Pushed Authorization Requests secondo quanto definito da OAuth 2.0 Pushed Authorization Requests (PAR) [RFC9126]
PGD	Piattaforma Gestione Deleghe
PKCE	Proof Key for Code Exchange
RP	Relying Party, sinonimo di Service Provider (Vedi anche acronimo SP)
SAML	Security Assertion Markup Language
SP	Fornitore di servizi digitali (Service Provider)

TM	Trust Mark
OTP	One-Time Password
FSE	Fascicolo Sanitario Elettronico
PNT	Piattaforma Nazionale Telemedicina
EDS	Ecosistema Dati Sanitari