AGID | Agenzia per l'Italia Digitale

# Regole tecniche per la gestione delle sessioni di autenticazione e del single sign-on

ai sensi dell'Allegato 2, Capitolo 1 delle "*Linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione*" ex art. 64-bis del D. Lgs. 7 marzo 2005, n. 82 e s.m.i.

Versione 1.0 del 7 giugno 2022

# 1. Introduzione

In attuazione di quanto previsto nell'Allegato 2 "Funzionalità del Punto di accesso telematico" delle **Linee guida sul Punto di accesso telematico ai servizi della Pubblica Amministrazione**, adottate da AgID ai sensi dell'articolo 71 del Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. (di seguito CAD) con Determinazione n. 598 in data 8 novembre 2021[1], le presenti regole tecniche individuano le modalità operative con cui il Punto di accesso telematico assicura:

- l'identificazione e l'autenticazione degli utenti finali dei servizi in rete resi disponibili dal Punto di accesso telematico, dipendente dallo stato delle identità rilasciate agli stessi utenti nel Sistema pubblico per la gestione delle identità digitali (SPID) di cui all'articolo 64 del CAD;
- la realizzazione del meccanismo di single sign-on tra il Punto di accesso telematico e i servizi in rete resi disponibili dai soggetti erogatori per dare inizio a specifici flussi o azioni dispositive integrate nell'esperienza dell'utente all'interno del Punto di accesso telematico.

Relativamente all'identificazione e all'autenticazione degli utenti finali realizzata dal Punto di accesso telematico, le presenti regole tecniche sono definite considerando il profilo di autenticazione individuato nelle Linee Guida OpenID Connect in SPID, adottate da AgID ai sensi dell'articolo 71 del CAD con Determinazione n. 616 del 2 dicembre 2021[2].

Il gestore del Punto di accesso telematico attua le presenti regole tecniche nella redazione della documentazione tecnica prevista nelle **Linee guida sul Punto di accesso telematico ai servizi della Pubblica Amministrazione**.

Nel rispetto delle presenti Regole tecniche e secondo gli accordi intercorrendi con il Ministero dell'Interno, il CieID server, quale IdP unico della federazione CIE, abilita l'utilizzo delle sessioni lunghe e del single sign-on mediante il punto di accesso telematico.

[1] https://trasparenza.agid.gov.it/index.php?id_oggetto=28&id_doc=123045
[2] https://trasparenza.agid.gov.it/index.php?id_oggetto=28&id_doc=123056

# 2. Riferimenti e sigle

## 2.1. Note alla lettura del documento

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici le presenti regole tecniche utilizzeranno le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUÒ» e «OPZIONALE», la cui interpretazione è descritta di seguito.

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

## 2.2. Riferimenti normativi

Sono riportati di seguito gli atti normativi di riferimento delle presenti regole tecniche.

| | |
|---|---|
| [CAD] | Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale"; |
| [GDPR] | 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati); |
| [Regolamentazione SPID] | D.P.C.M. 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese" e regolamentazione emessa ai sensi di tale decreto. |

## 2.3. Linee guida di riferimento

Di seguito sono elencate le linee guida emesse dall'AgID ai sensi dell'articolo 71 del CAD che sono richiamate nelle presenti regole tecniche.

| | |
|---|---|
| [LG PUNTO ACCESSO] | Linee guida sul Punto di accesso telematico ai servizi della |

| | |
|---|---|
| | Pubblica Amministrazione[3] |
| [LG SPID OIDC] | Linee Guida OpenID Connect in SPID[4] |
| [LG API SICUREZZA] | Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici[5] |
| [LG INTEROPERABILITÀ] | Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni[6] |

## 2.4. Acronimi, termini, definizioni

Di seguito si riportano i termini, gli acronimi e le definizioni che vengono utilizzati nelle presenti regole tecniche.

| | |
|---|---|
| AppPAT | L'applicazione utilizzata dall'utente finale per interagire con i servizi resi dal Punto di accesso telematico anche indicata come front-end nelle [LG PUNTO ACCESSO]. |
| IdP SPID | Identity Provider SPID accreditato da AgID. |
| PAT Backend | L'infrastruttura di back-end del Punto di accesso telematico di cui alle [LG PUNTO ACCESSO]. |
| Punto di accesso telematico | Il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri di cui all'articolo 64-bis del CAD. |
| Sessione di autenticazione | La sessione di autenticazione creata dal Punto di accesso telematico, generata a partire da un'identità SPID detenuta da uno dei IdP SPID. |
| Soggetti Erogatori | I soggetti che rendono fruibili i propri servizi in rete per il tramite del Punto di accesso telematico di cui alle [LG PUNTO ACCESSO]. |
| Utente finale | Il cittadino come definito nelle [LG PUNTO ACCESSO]. |

[3] https://www.agid.gov.it/sites/default/files/repository_files/lg_punto_accesso_telematico_servizi_pa_3112021.pdf
[4] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_openid_connect_in_spid.pdf
[5] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf
[6] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

# 3. Gestione delle sessioni di autenticazione

L'autenticazione realizzata dal *Punto di accesso telematico* prevede la generazione di una identità, mantenuta dallo stesso *Punto di accesso telematico*, derivata e dipendente da un'identità SPID emessa da uno degli IdP SPID.

Il *Punto di accesso telematico* nella gestione delle sessioni di autenticazione degli utenti finali DEVE assicurare:

- la creazione di una sessione di autenticazione generata a partire da un'identità SPID detenuta da uno dei IdP SPID;
- l'allineamento periodico della sessione di autenticazione con lo stato della identità SPID su cui la stessa è stata creata.

Nel processo per assicurare l'identificazione e autenticazione degli utenti finali del PAT si evidenziano:

- *AppPAT*, l'applicazione utilizzata dall'utente finale per interagire con i servizi resi dal *Punto di accesso telematico* anche indicata come front-end alle [LG PUNTO ACCESSO];
- *PAT Backend*, l'infrastruttura di back-end del *Punto di accesso telematico* di cui alle [LG PUNTO ACCESSO];
- *IdP SPID*, uno degli identity provider SPID accreditati da AgID.

Il processo per assicurare l'identificazione e autenticazione degli utenti finali del PAT prevede:

1) l'utente avvia l'*AppPAT* che, in maniera trasparente, DEVE interagire con *PAT Backend* per verificare l'esistenza di una sessione di autenticazione;
2) in relazione al risultato della verifica di cui al punto 1):
    a) se non esiste una sessione di autenticazione oppure il time-to-live del Refresh Token risulta scaduto presso il PAT Backend, allora:
        i) *AppPAT* DEVE richiedere l'autenticazione dell'utente presso uno degli *IdP SPID* e, a tal fine, *AppPAT* richiede all'utente finale:
            (1) la selezione dell'*IdP SPID* di proprio interesse;
            (2) di selezionare l'utilizzo di sessioni lunghe (scope = oidc e offline_access);

ii) *PAT Backend* DEVE avviare OpenID Connect Authorization Code Flow con l'*IdP SPID* selezionato dall'utente e, sulla base della selezione espresso dallo stesso, DEVE richiede l'instaurazione di una sessione lunga (scope = oidc e offline_access) o, viceversa, di una sessione non lunga (scope = oidc);

iii) al positivo completamento del processo di autenticazione realizzato dall'*IdP SPID*, *AppPAT* DEVE inoltrare l'Authorization Code al *PAT Backend* che DEVE creare una sessione di autenticazione interagendo con il Token Endpoint dello *IdP SPID* per scambiare l'authorization code con un ID Token e un Access Token e, nel caso di creazione di una sessione lunga, anche un Refresh Token;

iv) *PAT Backend* DEVE restituire la sessione di autenticazione alla *AppPAT* per concedere l'accesso all'utente finale;

b) se esiste una sessione di autenticazione e il time-to-live dell'Access Token non è ancora scaduto, allora *PAT Backend* DEVE restituire la sessione di autenticazione alla *AppPAT* per concedere l'accesso all'utente finale;

c) se esiste una sessione di autenticazione e il time-to-live dell'Access Token risulta scaduto, allora:

i) se l'utente non ha selezionato l'utilizzo di sessioni lunghe (scope = oidc), allora *PAT Backend* DEVE distrugge la sessione di autenticazione dandone evidenza alla *AppPAT* che non concede l'accesso all'utente finale e opera come nel precedente punto a);

ii) se l'utente ha selezionato l'utilizzo di sessioni lunghe (scope = oidc e offline_access), allora:

(1) se il time-to-live del Refresh Token risulta scaduto, allora *PAT Backend* DEVE distrugge la sessione di autenticazione dandone evidenza alla *AppPAT* che non concede l'accesso all'utente finale ed opera come nel precedente punto a);

(2) se il time-to-live del Refresh Token risulta non scaduto, allora allora *PAT Backend* DEVE aggiornare la sessione di autenticazione interagendo con Token Endpoint del *IdP SPID* per scambiare l'attuale Refresh Token con ID Token, Access Token e un nuovo Refresh Token; a valle del positivo aggiornamento dei token *PAT Backend* DEVE restituire la

sessione di autenticazione alla *AppPAT* per concedere l'accesso all'utente finale.

Si precisa che, nel processo per assicurare l'identificazione e l'autenticazione degli utenti finali del PAT indicato, si assume che:

- in tutti i casi in cui le interazioni tra *AppPAT* e *PAT Backend* con *IdP SPID* abbiano esito negativo (ad esempio Token Endpoint restituisce un errore nel consumare il Refresh Token presentato) allora *PAT Backend* DEVE distrugge la sessione di autenticazione dandone evidenza alla *AppPAT* che non concede l'accesso all'utente finale ed opera come nel precedente punto a;
- nel caso in cui l'*IdP SPID* non risponda (disservizio, non disponibilità), *PAT Backend* PUÒ mantenere la sessione di autenticazione attiva nei limiti della validità del Refresh Token, assumendosi ogni responsabilità derivante dalla sospensione o revoca dell'identità SPID sui cui la stessa sessioni di autenticazione è stata creata;
- gli *IdP SPID*, differentemente da quanto indicato nelle [LG SPID OIDC], DEVONO applicare la tecnica di Refresh Token Rotation, prevedendo che a ogni utilizzo di un Refresh Token lo stesso è sostituito da un nuovo Refresh Token la cui validità ha effetto dal momento dell'emissione, con time-to-live costante. Nello specifico gli *IdP SPID* emettono i token assicurando che il time-to-live dell'Access Token sia al massimo pari a 12 ore. Tanto premesso, nulla osta alla previsione di un time-to-live del Refresh Token pari al massimo a 270 giorni, individuati in base alle esigenze di usabilità ed accessibilità che sono state analizzate e rappresentate dal gestore del Punto di accesso telematico e diminuibili di concerto con gli IdP.

Nei seguenti paragrafi sono definite le azioni realizzate dal *Punto di accesso telematico* al fine di implementare l'indicato processo per assicurare l'identificazione e autenticazione degli utenti finali e i servizi per gestione delle sessioni di autenticazione rese disponibili agli utenti finali dallo stesso *Punto di accesso telematico*.

## 3.1. Autenticazione SPID degli utenti e creazione della sessione di autenticazione PAT

Il *Punto di accesso telematico* DEVE assicurare la creazione di una sessione di autenticazione PAT a partire da un'identità SPID detenuta da uno dei IdP SPID dando

seguito al processo di autenticazione previsto dalle [LG SPID OIDC]. Il livello di autenticazione SPID richiesto dal *Punto di accesso telematico* agli *IdP SPID* DEVE essere un'autenticazione di SPID di livello 2 (corrispondente a LoA3 della ISO-IEC 29115).

Il *Punto di accesso telematico* DEVE creare una nuova sessione di autenticazione PAT:

- in assenza di una sessione di autenticazione PAT per l'utente finale;
- nel caso in cui l'utente finale ha selezionato l'utilizzo di sessioni lunghe, se il time-to-live del Refresh Token associato a una sessione di autenticazione PAT risulta scaduto;
- nel caso in cui l'utente finale non abbia selezionato l'utilizzo di sessioni lunghe, se il time-to-live del Access Token associato a una sessione di autenticazione PAT risulta scaduto;
- in tutti i casi in cui le interazioni con l'*IdP SPID* diano esito negativo.

Il *Punto di accesso telematico* DEVE garantire all'utente finale la scelta di eventuali sessioni lunghe.

### 3.1.1. Ruoli e responsabilità

I ruoli e le responsabilità sono definite dalle [LG SPID OIDC], in cui si assume:

- User Agent, l'istanza della *AppPAT* utilizzata dall'utente finale per interagire con il *Punto di accesso telematico*;
- Relying Party, il *PAT Backend* che gestisce le sessioni di autenticazione degli utenti finali e l'accesso ai servizi resi disponibili dal *Punto di accesso telematico*;
- OpenID Provider, uno degli *IdP SPID*.

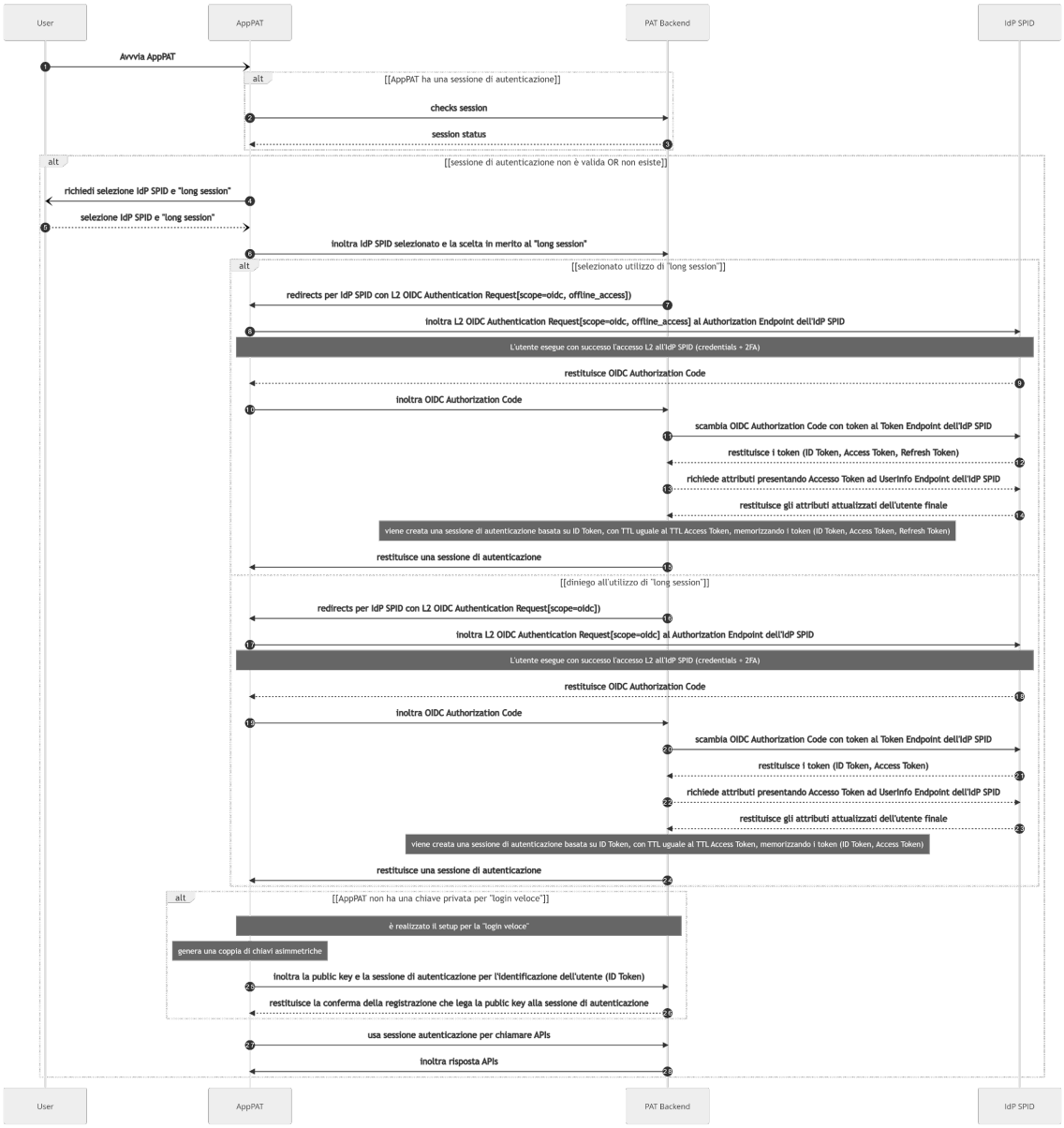
### 3.1.2. Interazioni realizzate

Le interazioni previste tra *AppPAT*, *PAT Backend* e *IdP SPID* per assicurare la creazione di una sessione di autenticazione a partire da un'identità SPID sono riportate nel seguente sequence diagram, nello stesso l'entità *User* rappresenta l'utente finale del *Punto di accesso telematico*.

Il sequence diagram evidenza che, in caso di riscontro da *PAT Backend* dello stato di assenza di una sessione di autenticazione valida (arrow da 1 a 3), è necessario che il *Punto*

*di accesso telematico* provveda ad all'autenticazione dell'utente per il tramite di uno degli *IdP SPID* in conformità alle [LG SPID OIDC] e nel dettaglio:

1. *AppPAT* DEVE chiedere all'utente finale di selezionare l'*IdP SPID* di suo interesse e, nel contempo, raccogliere la selezione da esso effettuata in merito all'utilizzo delle sessioni lunghe e inoltrare tali scelte a *PAT Backend* (arrow da 4 a 6);




2. In base alla selezione dell'utilizzo delle sessioni lunghe da parte dell'utente finale il flow prevede:
    a. se l'utente finale ha selezionato l'utilizzo di sessioni lunghe:

i. *PAT Backend* deve predisporre la Authentication Request, che *AppPAT* inoltrerà allo Authorization Endpoint del *IdP SPID* selezionato dall'utente finale, prevedendo il parametro ***scope*** valorizzato a ***oidc e offline_access*** e il parametro acr_values valorizzato a ***https://www.spid.gov.it/SpidL1 https://www.spid.gov.it/SpidL2*** (arrow 7 e 8);

ii. *IdP SPID* DEVE dare seguito al processo di autenticazione dell'utente ed in caso di esito positivo emettere un Authorization Code valido per sessioni lunghe per il *Punto di accesso telematico*[7] che *AppPAT* inoltrerà *PAT Backend* (arrow da 9 a 10);

iii. *PAT Backend* DEVE scambiare l'Authorization Code con ID Token, Access Token e Refresh Token, invocando il Token Endpoint del *IdP SPID* selezionato dall'utente finale, e successivamente DEVE utilizzare UserInfo Endpoint dello stesso *IdP SPID* per recuperare gli attributi dell'utente finale, al fine di creare la sessione di autenticazione sulla base dei token ricevuti e inoltrare a *AppPAT* l'avvenuta conclusione per permettere a quest'ultima di abilitare l'accesso ai servizi per l'utente finale (arrow da 11 a 15);

b. se l'utente finale non selezionato l'utilizzo di sessioni lunghe:

i. *PAT Backend* DEVE predisporre la Authentication Request, che *AppPAT* inoltrerà all'Authorization Endpoint del *IdP SPID* selezionato dall'utente finale, prevedendo il parametro ***scope*** valorizzato a ***oidc*** e il parametro acr_values valorizzato a ***https://www.spid.gov.it/SpidL1 https://www.spid.gov.it/SpidL2*** (arrow 16 e 17);

ii. *IdP SPID* DEVE dare seguito al processo di autenticazione dell'utente ed in caso di esito positivo emettere un Authorization Code valido per sessioni non lunghe per il *Punto di accesso telematico* che *AppPAT* inoltrerà *PAT Backend* (arrow 18 e 19);

iii. *PAT Backend* DEVE scambiare authorization code con ID Token e Access Token, invocando il Token Endpoint del *IdP SPID* selezionato dall'utente finale, e successivamente DEVE utilizzare UserInfo Endpoint dello stesso IdP SPID per recuperare gli attributi dell'utente

[7] In merito si ricorda che gli *IdP SPID* DEVONO applicare la tecnica di Refresh Token Rotation per i Refresh Token emessi per il Punto di accesso telematico.

finale, al fine di creare la sessione di autenticazione sulla base dei token ricevuti e inoltrare a *AppPAT* l'avvenuta conclusione per permettere a quest'ultima di abilitare l'accesso ai servizi per l'utente finale (arrow da 20 a 24);

3. Nel caso in cui *AppPAT* e *PAT Backend* non hanno inizializzato l'utilizzo di "login veloce", allora *AppPAT* genera una coppia di chiavi asimmetriche ed inoltra la public key al *PAT Backend*, *PAT Backend* associa la chiave public key all'utente (ID Token) e ne dà conferma ad *AppPAT* (arrow 25 e 26);
4. *AppPAT* utilizza la sessione di autenticazione per accedere alle APIs del *PAT Backend* per dare accesso ai servizi del *Punto di accesso telematico* all'utente finale (arrow 27 e 28).

Le API realizzate dai soggetti interessati per dare seguito alle interazioni previste sono implementate nel rispetto delle [LG INTEROPERABILITÀ].

### 3.1.3. Tracciatura delle interazioni

Fatti salvi gli obblighi di tracciatura previsti per *IdP SPID* così come individuati dal quadro regolatorio del SPID e, nello specifico, dalle [LG SPID OIDC], il *Punto di accesso telematico*, e nello specifico *PAT Backend* DEVE assicurare la tracciatura delle richieste di login effettuate da *AppPAT* comprensivo della selezione effettuata dall'utente finale in merito all'utilizzo delle sessioni lunghe, i cui tempi di conservazione sono individuati dal gestore del *Punto di accesso telematico* in coerenza con le [LG PUNTO ACCESSO] e nel rispetto di quanto prescritto al paragrafo 4.1. Tracciature identity provider del Regolamento recante le regole tecniche ex articolo 4, comma 2, D.P.C.M. 24 ottobre 2014.

Nello specifico delle autenticazioni realizzate tramite "login veloce" PAT Backend DEVE tracciare gli eventi e gli oggetti scambiati per abilitare la creazione di una sessione di autenticazione a valle della verifica della firma prevista per il "challenge" tra AppPAT e PAT Backend.

### 3.1.4. Misure di sicurezza adottate

Fatti salvi impedimenti imputabili al dispositivo utilizzato dall'utente finale per istanziare la *AppPAT* il *Punto di accesso telematico* DEVE assicurare lo scambio di materiale crittografico

generato da AppPAT e inoltrato a *PAT Backend* per assicurare il signed challenge tra *AppPAT* e *PAT Backend* nelle successive interazioni tra esse (in breve la "login veloce").

Il PAT Backend DEVE assicurare che in ogni momento temporale per uno specifico utente finale lo stesso possa abilitare un solo dispositivo per l'utilizzo di AppPAT.

Le comunicazioni realizzate per dare seguito alle interazioni previste tra i soggetti coinvolti applicano le indicazioni in merito alla sicurezza a livello di trasporto indicate nelle [LG API SICUREZZA].

Relativamente agli ID token, Access Token e Refresh Token resi persistenti dal PAT backend e alle public key generate da AppPAT e resi persistenti su PAT backend, lo stesso PAT backend DEVE operare nel rispetto delle "Disposizioni in materia di sicurezza e protezione dei dati personali" indicate nelle [LG PUNTO ACCESSO] assicurando per gli stessi:

- l'integrità e immodificabilità provvedendo ad applicare tutte le misure tecniche/organizzative necessarie;
- l'utilizzo nei limiti della realizzazione della autenticazione SPID degli utenti e creazione della sessione di autenticazione PAT.

Relativamente alle private key generate da AppPAT e da essa rese persistenti, l'AppPAT DEVE utilizzare dei meccanismi di isolamento hardware, dove possibile, per mitigare la possibilità che le private key siano estratte dal dispositivo.

## 3.2. Autenticazioni degli utenti in presenza di sessione di autenticazione PAT

Nel caso in cui l'utente finale abbia selezionato l'utilizzo di sessioni lunghe, il *Punto di accesso telematico* è responsabile dell'autenticazione degli utenti finali per cui è stata creata una sessione di autenticazione nelle modalità indicate al paragrafo 3.1.

Il *Punto di accesso telematico* DEVE assicurare l'allineamento delle sessioni di autenticazione con le identità SPID sui cui le stesse sono state create:

- nel caso in cui l'utente finale abbia selezionato l'utilizzo di sessioni lunghe, se il time-to-live del Access Token associato ad una sessione di autenticazione PAT risulti scaduto e il time-to-live del Refresh Token associato alla stessa sessione di autenticazione PAT risulti ancora valido.

Il *Punto di accesso telematico* DEVE assicurare l'accesso costante dell'utente finale all'informativa sul trattamento dei dati personali, che dovrà concernere anche la gestione delle sessioni lunghe.

### 3.2.1. Ruoli e responsabilità

Nel presente contesto le entità coinvolte sono:

- l'istanza della *AppPAT* utilizzata dall'utente finale per interagire con il *Punto di accesso telematico*;
- il *PAT Backend* che gestisce le sessioni di autenticazione degli utenti finali e l'accesso ai servizi resi disponibili dal *Punto di accesso telematico*;
- uno degli *IdP SPID* che rende disponibile lo stato delle identità SPID utilizzate per la creazione delle sessioni di autenticazione.

Le entità *AppPAT* e *PAT Backend* sono responsabili dell'autenticazione dell'utente finale e l'associazione alla sessione di autenticazione precedentemente creata per lo stesso utente.

Gli *IdP SPID* sono responsabili di fornire lo stato delle identità SPID di propria competenza e DEVONO assicurare che UserInfo Endpoint restituisca gli attributi dell'utente associato alle identità SPID attualizzati al momento della richiesta da parte del *Punto di accesso telematico*.

La verifica dello stato dell'identità SPID su cui una sessione di autenticazione è stata creata è realizzata da *PAT Backend* che DEVE utilizzare il Token Endpoint del *IdP SPID* interessato per scambiare l'attuale Refresh Token con ID Token, Access Token e un nuovo Refresh Token.

Gli *IdP SPID*, nel caso in cui l'identità SPID associata ad un Refresh Token risulti sospesa o revocata, DEVONO rispondere con un errore sulla base della lista di codici di errori riconosciuti dal protocollo.

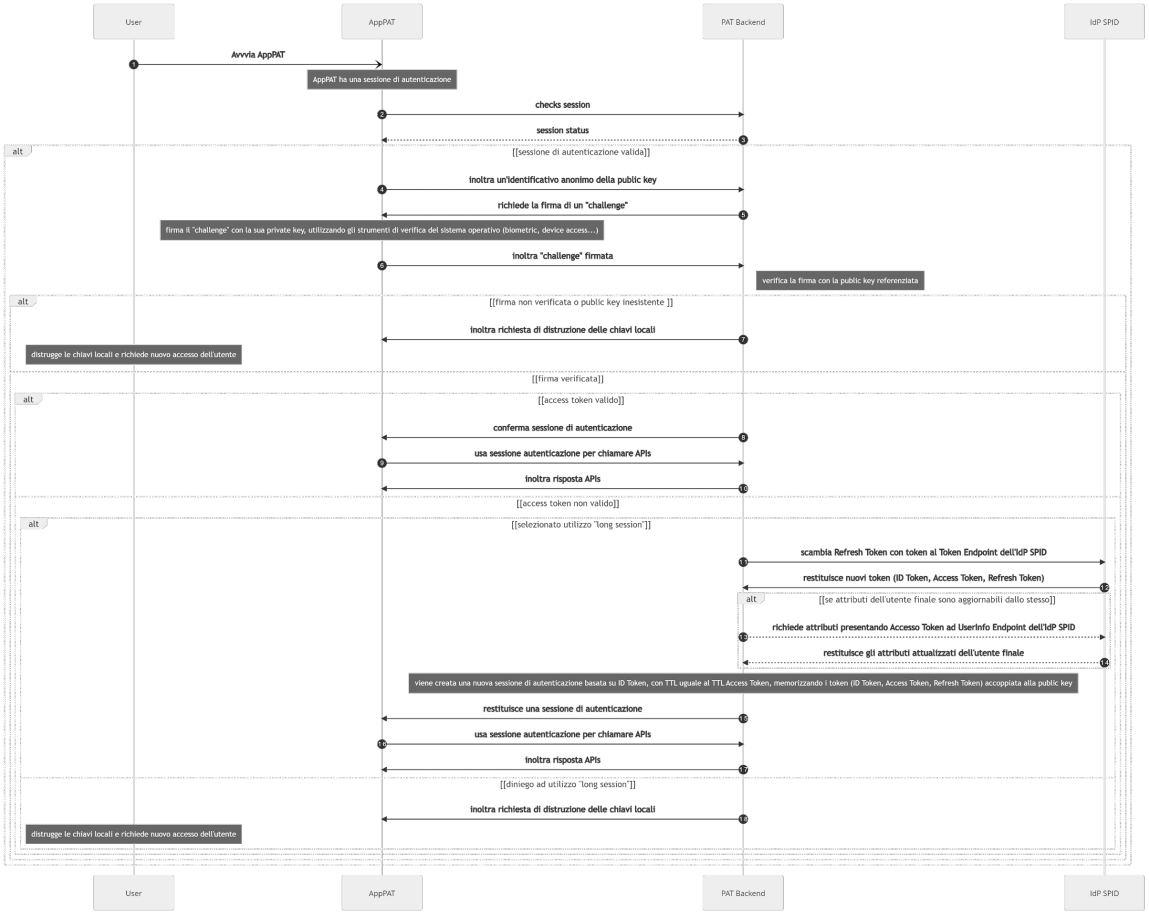
Il *PAT Backend,* nel caso di risposta con errore da parte del *IdP SPID,* DEVE distruggere la sessione di autenticazione dandone evidenza alla *AppPAT* che non concede l'accesso all'utente finale ed opera come al precedente paragrafo 3.1.

### 3.2.2. Interazioni realizzate

Le interazioni previste tra *AppPAT*, *PAT Backend* e *IdP SPID* per assicurare l'autenticazione di un utente finale, nell'ipotesi in cui l'utente finale ha selezionato l'utilizzo di sessioni lunghe, in presenza di Refresh Token non ancora scaduto sono riportate nel seguente sequence diagram, nello stesso l'entità *User* rappresenta l'utente finale del *Punto di accesso telematico*.

Il sequence diagram evidenza che, in caso di riscontro da *PAT Backend* dello stato di presenza di una sessione di autenticazione valida (arrow da 1 a 3), il *Punto di accesso telematico* provveda ad all'autenticazione dell'utente e nel dettaglio:

1. *AppPAT* provvede ad inoltrare un riferimento alla public key in suo possesso e firma la "challenge" inoltrata da *PAT Backend* (arrow da 4 a 6);
2. In base alla verifica della firma realizzata da *PAT Backend*:
    a. se la firma non è valida o la public key non risulta presente:
        i. *PAT Backend* richiede la distruzione delle chiavi a *AppPAT* (arrow 7) e *AppPAT* avvia una nuova autenticazione SPID (vedi 3.1);
    b. se la firma è valida, in relazione alla validità dell'Access Token riferito alla sessione di autenticazione:
        i. se l'Access Token è ancora valido, *AppPAT* utilizza la sessione di autenticazione per accedere alle APIs del *PAT Backend* per dare accesso ai servizi del *Punto di accesso telematico* all'utente finale (arrow da 8 a 10);




ii. se l'Access Token non è ancora valido, in base alla selezione dell'utilizzo delle "long session" dato dall'utente finale:

   a. se l'utente ha selezionato le "long session", allora *PAT Backend* scambia il Refresh Token associato alla sessione di autenticazione con ID Token, Access Token e un nuovo Refresh Token, invocando il Token Endpoint del *IdP SPID* selezionato dall'utente finale, e successivamente DEVE utilizzare UserInfo Endpoint dello stesso IdP SPID per recuperare gli attributi dell'utente finale se gli stessi sono modificabili da quest'ultimo, al fine di crea la nuova sessione di autenticazione sulla base dei token ricevuti e inoltra a *AppPAT* l'avvenuta conclusione per permettere alla stessa di utilizzare la sessione di autenticazione per accedere alle APIs del *PAT Backend* per dare accesso ai servizi del *Punto di accesso telematico* all'utente finale (arrow da 11 a 15);

b. se l'utente non ha selezionato le “long session”, *PAT Backend* richiede la distruzione delle chiavi a *AppPAT* (arrow 16) e *AppPAT* avvia una nuova autenticazione SPID (vedi 3.1).

Le API realizzate dai soggetti interessati per dare seguito alle interazioni previste sono implementate nel rispetto delle [LG INTEROPERABILITÀ].

### 3.2.3. Tracciatura delle interazioni

Fatti salvi gli obblighi di tracciatura previsti per *IdP SPID* così come individuati dal quadro regolatorio del SPID, e nello specifico dalle [LG SPID OIDC], il *Punto di accesso telematico*, e nello specifico *PAT Backend* DEVE assicurare la tracciatura delle operazioni di autenticazione realizzate sulla base dell'identificazione realizzata da *AppPAT* i cui tempi di conservazione sono individuati dal gestore del *Punto di accesso telematico* in coerenza con le [LG PUNTO ACCESSO] e nel rispetto di quanto prescritto al paragrafo 4.1. Tracciature identity provider del Regolamento recante le regole tecniche ex articolo 4, comma 2, DPCM 24 ottobre 2014.

Nello specifico delle autenticazioni realizzate tramite “login veloce” PAT Backend DEVE tracciare gli eventi e gli oggetti scambiati per dare seguito alla verifica della firma prevista per il “challenge” tra AppPAT e PAT Backend.

### 3.2.4. Misure di sicurezza adottate

Fatti salvi impedimenti imputabili al dispositivo utilizzato dall'utente finale per istanziare la *AppPAT* il *Punto di accesso telematico* DEVE assicurare in maniera alternativa i seguenti meccanismo di identificazione dell'utente finale:

1. tramite riconoscimento biometrico dell'utente finale, per il tramite degli strumenti messi a disposizione dispositivo utilizzato dallo stesso;
2. in assenza di supporto al biometrico da parte del dispositivo o della scelta dell'utente finale di non usarlo, tramite meccanismo di sblocco registrato dallo stesso in fase di inizializzazione del *AppPAT* o per successive modifiche realizzate tramite la stessa *AppPAT*.

AppPAT PUÒ utilizzare meccanismi di sblocco, quali PIN, Password o Pattern (segno di sblocco) implementati dalla stessa AppPAT o recuperati dalle funzionalità del sistema operativo ospitante.

*AppPAT* DEVE permettere all'utente finale di poter modificare in ogni momento il meccanismo di identificazione.

*AppPAT*, in relazione a tentativi illeciti di identificazione, come ad esempio brute force attack, DEVE applicare le necessarie contromisure, ad esempio nel caso di utilizzo di del meccanismo di sblocco deve limitare il numero di inserimenti consecutivi scorretti.

Le contromisure adottate dal gestore del *Punto di accesso telematico* sono oggetto della valutazione d'impatto sulla protezione dei dati personali di cui alle [LG PUNTO ACCESSO].

Le comunicazioni realizzate per dare seguito alle interazioni previste tra i soggetti coinvolti applicano le indicazioni in merito alla sicurezza a livello di trasporto indicate nelle [LG API SICUREZZA].

Relativamente agli ID token, Access Token e Refresh Token resi persistenti dal PAT backend e alle public key generate da AppPAT e resi persistenti su PAT backend, lo stesso PAT backend DEVE operare nel rispetto delle "Disposizioni in materia di sicurezza e protezione dei dati personali" indicate nelle [LG PUNTO ACCESSO] assicurando per gli stessi:

- l'integrità e immodificabilità provvedendo ad applicare tutte le misure tecniche/organizzative necessarie;
- l'utilizzo nei limiti della realizzazione della autenticazioni degli utenti in presenza di sessione di autenticazione PAT.

Relativamente alle private key generate da AppPAT e da essa rese persistenti, la stessa AppPAT DEVE utilizzare dei meccanismi di isolamento hardware, dove possibile, per mitigare la possibilità che le private key siano estratte dal dispositivo.

## 3.3. Servizi per la gestione delle sessioni di autenticazione PAT

In quanto segue sono riportati i servizi assicurati dal gestore del *Punto di accesso telematico* per permettere agli utenti finali di gestire, in caso di perdita del controllo del *AppPT* o del dispositivo utilizzato per istanziare la *AppPAT*, gli accessi realizzati e le eventuali sessioni di autenticazione ancora attive.

### 3.3.1. Consultazione degli accessi realizzati

Il servizio di consultazione degli accessi eseguiti è reso agli utenti finali all'interno di *AppPAT* a valle dell'abilitazione all'accesso ai servizi nei modi indicati ai precedenti paragrafi 3.1 e 3.2.

Il servizio di consultazione degli accessi realizzato, a valle dell'autenticazione dell'utente finale, rende disponibile l'elenco degli accessi al massimo per i tempi di conservazione della tracciatura delle interazioni indicati ai precedenti paragrafi 3.1.3 e 3.2.3 .

### 3.3.2. Distruzione delle sessioni di autenticazione PAT

Il *Punto di accesso telematico* assicura agli utenti finali la possibilità di dare seguito alla distruzione, in breve logout, delle sessioni di autenticazione generate.

Il *Punto di accesso telematico* DEVE assicurare:

- logout tramite *AppPAT*, permettendo all'utente finale di effettuare il logout dalla sessione di autenticazione generate, l'autenticazione dell'utente finale è realizzata nei modi indicati ai paragrafi 3.1 e 3.2;
- logout remoto, in caso di perdita del dispositivo, il gestore del *Punto di accesso telematico* rende disponibile un canale alternativo ad *AppPAT* per permettere all'utente finale di effettuare logout dalle sessione di autenticazione generate, l'autenticazione dell'utente finale è realizzata attraverso autenticazione SPID di livello 1 ed eventuali successiva conferma attraverso i canali di comunicazione con il *Punto di accesso telematico*.

# 4. Single sign-on con i servizi dei soggetti erogatori

Il *Punto di accesso telematico* DEVE implementare e rendere disponibile ai *Soggetti Erogatori* un meccanismo di single sign-on che, nell'ambito delle sessioni di autenticazione generate dal *Punto di accesso telematico* nei modi indicati ai precedenti paragrafi 3.1 e 3.2, permette di abilitare l'accesso dell'utente finale ai servizi resi dagli stessi *Soggetti Erogatori* per il tramite del *Punto di accesso telematico*.

Il meccanismo di single sign-on realizzato dal *Punto di accesso telematico* DEVE prevedere la generazione di un token a partire dalla sessione di autenticazione dell'utente finale per trasportare l'identità dello stesso utente finale presso uno dei servizi di un *Soggetto Erogatore*.

Il *Punto di accesso telematico DEVE* abilitare il meccanismo di single sign-on per i soli *Soggetti Erogatori* censiti nei modi indicati dalle [LG PUNTO ACCESSO] che hanno indicato i servizi per cui richiedono l'utilizzo del meccanismo di single sign-on e i relativi attributi richiesti.

I *Soggetti Erogatori* DEVONO implementare il meccanismo di single sign-on nel rispetto delle specifiche tecniche emanate dal gestore del *Punto di accesso telematico*.

Il meccanismo di single sign-on PUÒ essere utilizzato sia in contesti web che in contesti programmatici.

## 4.1. Integrazione Punto di accesso telematico e soggetti erogatori

Il *Punto di accesso telematico* DEVE assicurare:

- la creazione di un token che trasporta l'identità dell'utente finale (ID Token), emesso per il singolo Soggetto Erogatore;
- la firma del token emesso per assicurare l'integrità, immodificabilità e certezza della fonte.

### 4.1.1. Ruoli e responsabilità

Nel processo implementato dal meccanismo di single sign-on si evidenziano:

- *AppPAT*, l'applicazione utilizzata dall'utente finale per interagire con i servizi resi dal Punto di accesso telematico anche indicata come front-end alle [LG PUNTO ACCESSO];
- *PAT Backend*, l'infrastruttura di back-end del Punto di accesso telematico di cui alle [LG PUNTO ACCESSO], che svolge anche il ruolo di OpenID Provider
- *Servizio del Soggetto Erogatore*, il servizio terzo che vuole offrire l'accesso alle sue funzionalità dell'utente finale tramite meccanismo di single sign-on reso disponibile dal *Punto di accesso telematico*.

Il meccanismo di single sign-on reso disponibile dal *Punto di accesso telematico* è realizzato attraverso l'implementazione del OpenID Connect Implicit Flow in cui si assume la presenza di una sessione di autenticazione valida generata nei modi indicati al paragrafo 3.1 e 3.2, in cui:

- *Servizio del Soggetto Erogatore* svolge il ruolo di Relying Party;
- *AppPAT* svolge il ruolo dello User Agent dell'utente finale;
- *PAT Backend* svolge il ruolo di OpenID Provider.

Per quanto concerne la protezione dei dati personali con riferimento al single sign-on, il gestore del PAT e il Soggetto Erogatore trattano i dati personali in qualità di titolari autonomi.

### 4.1.2. Interazioni realizzate

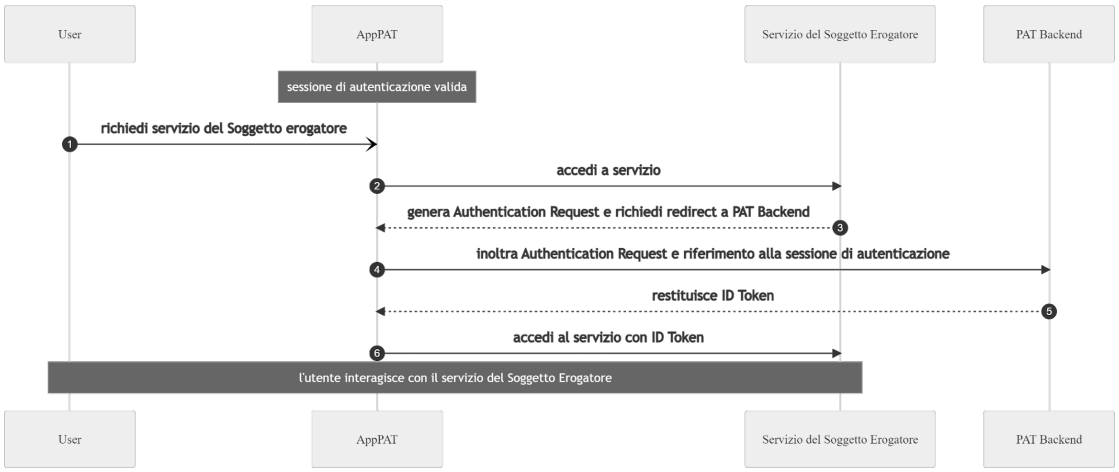
Le interazioni previste tra *AppPAT*, *PAT Backend* e *Servizio del Soggetto Erogatore* per assicurare l'accesso dell'utente finale tramite meccanismo di single sign-on reso disponibile dal *Punto di accesso telematico*, in cui si assume la creazione di una sessione di autenticazione nei modi indicati ai paragrafi 3.1 e 3.2, sono riportate nel seguente sequence diagram, nello stesso l'entità *User* rappresenta l'utente finale del *Punto di accesso telematico*.

Il sequence diagram evidenza che, in presenza di una sessione di autenticazione valida, l'utente finale richiede ad *AppPAT* di accedere ad un servizio di un *Soggetto Erogatore* (arrow 1 e 2).

Il Servizio del *Soggetto Erogatore* genera Authentication Request che *AppPAT* inoltra, congiuntamente al riferimento della sessione di autenticazione *PAT Backend* (arrow 3 e 4).

*PAT Backend*, a valle della verifica di validità della sessione di autenticazione, emette un ID Token destinato al Servizio del *Soggetto Erogatore* e lo inoltra ad *AppPAT* (arrow 5).

*AppPAT* accede al Servizio del *Soggetto Erogatore* presentando l'ID Token ricevuto (arrow 6), ed in caso di verifica positiva del contenuto dell'ID Token e della firma apposta dal *PAT Backend*, l'utente finale interagisce con lo stesso servizio.




Le API realizzate dai soggetti interessati per dare seguito alle interazioni previste sono implementate nel rispetto delle [LG INTEROPERABILITÀ].

### 4.1.3. Tracciatura delle interazioni

Il *Punto di accesso telematico* e, nello specifico, *PAT Backend* DEVONO assicurare la tracciatura delle Authentication Request generate dai Servizi dei *Soggetti Erogatori* e, per esse, i relativi ID Token emessi. I tempi di conservazione sono individuati dal gestore del *Punto di accesso telematico* in coerenza con le [LG PUNTO ACCESSO] e nel rispetto di quanto prescritto al paragrafo 4.1. Tracciature identity provider del Regolamento recante le regole tecniche ex articolo 4, comma 2, DPCM 24 ottobre 2014.

### 4.1.4. Misure di sicurezza adottate

Il meccanismo di single sign-on implementato dal Punto di accesso telematico è realizzato all'interno di un sistema chiuso in cui le parti coinvolte, Punto di accesso telematico e servizi dei *Soggetti Erogatori*, sono identificati a priori attraverso il censimento realizzato per il tramite il Back office dedicato ai Soggetti erogatori previsto nelle [LG PUNTO ACCESSO].

Il *Punto di accesso telematico* e i *Soggetti Erogatori* DEVONO utilizzare Back office dedicato ai Soggetti erogatori previsto nelle [LG PUNTO ACCESSO] per scambiarsi il materiale crittografico necessario all'identificazione delle parti coinvolte nelle interazioni indicate al precedente paragrafo 4.1.2.

L'ID Token emessi dal *Punto di accesso telematico* DEVONO essere dei JSON Web Token[8] includenti almeno i claims:

- issued at (iat), per identificare il momento temporale di emissione del token;
- expiration time (exp), per identificare il momento temporale oltre cui il token non è più valido;
- issuer (iss), il soggetto per ha emesso il token, nello specifico *PAT Backend*;
- audience (aud), il destinatario per cui il token è stato emesso, nello specifico il servizio del Soggetto Erogatore;
- il precedente claim expiration time (exp) è valorizzato al massimo a 5 minuti.

Il PAT Backend DEVE popolare l'ID Token con i soli claim relativi agli attributi all'utente finale richiesti dal Soggetto Erogatore nella Authentication Request limitatamente ai soli claim relativi agli attributi dell'utente finale indicati dall'IdP SPID al momento dell'autenticazione e agli altri attributi dichiarati dall'utente finale tramite PAT. .

I *Soggetti Erogatori* DEVONO richiedere l'insieme minimo di claim relativi agli attributi dell'utente finale per ridurre il trattamento ai soli dati strettamente necessari per la fornitura dei servizi offerti, nel rispetto del principio di minimizzazione dei dati ai sensi dell'art. 5, par. 1, lett. c) del GDPR.

[8] https://datatracker.ietf.org/doc/html/rfc7519

Le comunicazioni realizzate per dare seguito alle interazioni previste tra i soggetti coinvolti applicano le indicazioni in merito alla sicurezza a livello di trasporto indicate nelle [LG API SICUREZZA].

Relativamente alla tracciatura si evidenzia che:

- Authentication Request e informazioni contenute nel payload dell'ID Token DEVONO essere rese persistenti dal PAT Backend;
- Authentication Request e ID Token firmato da PAT Backend DEVONO essere resi persistenti dai Soggetti Erogatori;

operando nel rispetto delle "Disposizioni in materia di sicurezza e protezione dei dati personali" indicate nelle [LG PUNTO ACCESSO] ed assicurando per gli stessi:

- l'integrità e immodificabilità provvedendo ad applicare tutte le misure tecniche/organizzative necessarie;
- l'utilizzo nei limiti della realizzazione del single sign-on con i servizi dei soggetti erogatori.

## 4.2. Servizi per la gestione degli accessi ai servizi realizzati tramite SSO

In quanto segue sono riportati i servizi assicurati dal gestore del *Punto di accesso telematico* per permettere agli utenti finali di avere contezza degli accessi realizzati tramite il meccanismo di single sign-on.

### 4.2.1. Consultazione degli accessi realizzati tramite SSO

Il servizio di consultazione degli accessi eseguiti tramite il meccanismo di single sign-on è reso agli utenti finali all'interno di *AppPAT* a valle dell'abilitazione all'accesso ai servizi nei modi indicati ai precedenti paragrafi 3.1 e 3.2.

Il servizio di consultazione degli accessi realizzato, a valle dell'autenticazione dell'utente finale, rende disponibile l'elenco degli accessi al massimo per i tempi di conservazione della tracciatura delle interazioni indicati al precedente paragrafo 4.1.3.

## 4.3. Violazioni di dati personali

Ferme le disposizioni in materia di sicurezza e protezione dei dati personali di cui al Capitolo 7 delle **Linee guida sul Punto di accesso telematico ai servizi della Pubblica Amministrazione**, si precisa quanto segue con riferimento alla prevenzione e alla gestione di eventuali violazioni di dati personali.

Il gestore del PAT DEVE:

a) adottare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, sorvegliare e tracciare l'accesso e le attività dei propri utenti per il tempo strettamente necessario e anche al fine di tutelare la protezione dei dati personali secondo quanto definito dagli artt. 25, 29 e 32 del GDPR, informando tempestivamente i Soggetti Erogatori in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati e stabilendone le modalità all'interno della valutazione d'impatto sulla protezione dei dati personali;
b) in caso di violazione dei dati personali, procedere all'eventuale notifica al Garante per la protezione dei dati personali e, ove necessario, alla comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR.

Il Soggetto Erogatore DEVE garantire:

a) la conformità del servizio erogato alla normativa vigente, anche in tema di protezione dei dati personali sin dalla progettazione e per impostazione predefinita, effettuando un'analisi del rischio e, qualora sussistano le condizioni di cui agli artt. 35 e 36 del GDPR, altresì la valutazione d'impatto sulla protezione dei dati personali e l'eventuale consultazione preventiva;
b) l'adozione di misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, sorvegliare e tracciare l'accesso e le attività dei propri utenti per il tempo strettamente necessario e al solo fine di tutelare la protezione dei dati personali secondo quanto definito dagli artt. 25, 29 e 32 del GDPR, informando tempestivamente il gestore del PAT in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati;
c) in caso di violazione dei dati personali, l'eventuale notifica al Garante per la protezione dei dati personali e, ove necessario, la comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR.