

Termini aggiuntivi per la funzionalità *Single Sign On* “SSO”

V. 1.0 - 31 marzo 2026

1. OGGETTO DEI TERMINI AGGIUNTIVI E EFFICACIA

Il presente Addendum (o Termini Aggiuntivi) disciplina, in via specifica e integrativa rispetto all'Accordo, l'utilizzo della funzionalità di “Single Sign On” (SSO) dell'app IO, che consente all'utente finale, già autenticato su IO, di accedere ai servizi digitali ospitati sui Sistemi dell'Ente senza necessità di una ulteriore identificazione tramite SPID o CIE.

Il presente Addendum si applica esclusivamente agli Enti che abbiano aderito all'Accordo per l'uso dell' app IO e che abbiano abilitato, per il tramite del Portale di Back-Office, ovvero in caso di indisponibilità, per il tramite del Service Management, uno o più servizi alla funzionalità di SSO.

L'abilitazione di anche solo un servizio a SSO costituisce accettazione integrale e automatica delle disposizioni del presente Addendum, che diviene parte integrante e sostanziale dell'Accordo a decorrere dalla data di effettiva attivazione della funzionalità.

L'Ente prende atto che l'abilitazione dei servizi a SSO costituisce presupposto di previa presa visione e accettazione della Documentazione Tecnica e del presente Addendum, disponibili sul sito istituzionale della Società e sul Portale di Back-Office [al presente link](#).

2. DEFINIZIONI, PREVALENZA E RINVIO

2.1. Salvo diversamente stabilito, i termini in maiuscolo contenuti nei presenti Termini Aggiuntivi hanno il significato a loro attribuito nell'Accordo.

Ai fini dei presenti Termini Aggiuntivi, per “Sistemi dell'Ente” si intende l'insieme dei sistemi e delle componenti tecnologiche messe a disposizione dall'Ente per l'offerta dei propri servizi al pubblico.

Ai fini dei presenti Termini Aggiuntivi, il termine “SSO” indica un meccanismo di autenticazione che permette ad un Utente che si è connesso all'app IO, con una sessione attiva, attraverso una versione compatibile dell'app, di accedere a un servizio proseguendo l'esperienza sui Sistemi dell'Ente a partire dalla scheda Servizio o da un messaggio, senza necessità di una ulteriore identificazione. A fini di chiarezza, SSO non sarà considerato disponibile se un Utente (a) non ha installato l'app IO sul suo dispositivo, (b) non è connesso all'app IO con una sessione attiva, o (c) non ha una connessione Internet.

Ai fini dei presenti Termini Aggiuntivi, il termine “Proof of Possession” indica la chiave

crittografica generata e tenuta segreta dal dispositivo all'interno del Sottosistema sicuro (privata) che corrisponde a una chiave pubblica il cui hash è memorizzato, insieme agli attributi identificativi del possessore, all'interno della SAML Response, rilasciata e firmata dall'Identity Provider in fase di identificazione su IO.

2.2. Per tutto quanto non espressamente previsto nei presenti Termini Aggiuntivi, si applicano i termini dell'Accordo. In caso di discrepanza tra le previsioni dei presenti Termini Aggiuntivi e le previsioni contenute negli altri documenti dell'Accordo, si applicherà il seguente ordine di prevalenza:

- i) i presenti Termini Aggiuntivi;
- ii) i T&C dell'Accordo IO base.

3. RUOLO E OBBLIGHI DELLE PARTI NELL'AMBITO DELLA FUNZIONALITÀ SSO

3.1. PagoPA (o Società), in qualità di Gestore del Punto di Accesso Telematico ("PAT") ai sensi dell'art. 64-bis del CAD e delle Linee Guida sul Punto di Accesso Telematico ("LLGG IO"), opera esclusivamente quale OpenID Provider nell'ambito della funzionalità SSO. In tale contesto, PagoPA è responsabile:

- a) dell'identificazione dell'Utente sull'app IO secondo le modalità previste dalla normativa vigente;
- b) dell'emissione e della firma digitale dell'ID Token contenente gli attributi dell'Utente richiesti dall'Ente Erogatore;
- c) della gestione della sessione di autenticazione sull'app IO e del corretto funzionamento dei meccanismi di federated identity, secondo le specifiche OIDC e le Regole tecniche SSO;
- d) della tracciatura delle Authentication Request generate dai servizi dei Soggetti erogatori cui i singoli Utenti accedono mediante il meccanismo di federated identity e dei relativi ID Token generati dalla componente SSO.

PagoPA non assume:

- a) alcun ruolo nell'erogazione dei servizi dell'Ente Erogatore;
- b) alcuna responsabilità in ordine a procedimenti amministrativi, ai contenuti, agli esiti o agli effetti giuridici dei servizi accessibili tramite SSO;
- c) alcun obbligo di verifica circa la legittimità, adeguatezza o conformità dei servizi resi dall'Ente.

Resta inteso che l'attività di PagoPA è limitata alla sola gestione del canale tecnico di accesso e non comporta in alcun caso la delega di funzioni amministrative né di assunzione di responsabilità circa i contenuti del servizio.

L'attività svolta dalla Società ai sensi dei presenti Termini Aggiuntivi deve intendersi limitata alle attività di sviluppo e assistenza ivi indicate. Per tutto quanto non espressamente disciplinato dai presenti Termini Aggiuntivi si applicano i termini e condizioni dell'Accordo.

3.2. L'Ente si impegna a fornire piena collaborazione alla Società affinché la stessa possa

svolgere le attività di cui ai presenti Termini Aggiuntivi, anche facilitando il dialogo e confronto con i soggetti coinvolti nell'esecuzione dell'Accordo.

L'Ente si impegna, altresì, a:

- a) censire correttamente sul Portale Back-Office di IO tutti i servizi accessibili tramite SSO, fornendo ogni dato e/o informazione richiesta dalla Società (i.e., redirect URI, chiavi pubbliche e configurazioni conformi alle specifiche tecniche);
- b) implementare i controlli tecnici idonei a verificare la validità, integrità e provenienza dell'ID Token (verifica della firma apposta dal Gestore) nonché la Proof of Possession (verifica della corrispondenza con la chiave pubblica memorizzata sotto forma di hash nella SAML Response) prima di consentire l'accesso al/ai servizi;
- c) assicurare la tracciabilità delle richieste di autenticazione e degli ID Token ricevuti, nel rispetto delle misure di sicurezza e di conservazione previste dalla normativa applicabile;
- d) utilizzare SSO esclusivamente per i servizi compatibili con il livello di sicurezza offerto dal meccanismo di federated identity.

3.3. L'Ente Erogatore è, altresì, responsabile:

- a) della corretta conformità normativa dei servizi erogati;
- b) della verifica dell'età dell'Utente ai fini dell'accesso ai servizi;
- c) della corretta informazione all'Utente in merito al trattamento dei dati personali;
- d) della valutazione dei rischi e, ove necessario, dello svolgimento della valutazione d'impatto sulla protezione dei dati per i trattamenti di propria competenza.

4. ASSISTENZA E RESPONSABILITÀ DELLE PARTI NELL'AMBITO DELLA FUNZIONALITÀ SSO

Fermo restando l'impegno a collaborare in buona fede e ad individuare ogni strumento utile ad evitare disallineamenti informativi, le Parti convengono che l'assistenza (comprensiva delle attività di debug, troubleshooting e incident response) agli Utenti e le rispettive responsabilità delle Parti in tal senso avverrà sulla base dei rispettivi perimetri di controllo sui Sistemi delle Parti, secondo quanto previsto di seguito:

- a) tramite il proprio servizio helpdesk, la Società offre assistenza di primo e secondo livello per le fasi di identificazione e autenticazione alla Piattaforma IO (SPID/CIE), per problematiche dipendenti esclusivamente dal funzionamento dell'app IO o della Piattaforma IO, nonché della Funzionalità di SSO limitatamente al perimetro della app IO e della Piattaforma IO. In tali casi, l'assistenza fornita dalla Società è limitata alle problematiche afferenti alla Piattaforma IO e all'app IO e non comprende in alcun caso attività di diagnosi, intervento o supporto sui Sistemi dell'Ente o sui Servizi al cittadino offerti da quest'ultimo tramite la Piattaforma IO;
- b) la Società indirizza gli Utenti dell'app IO verso i canali messi a disposizione dall'Ente e dagli enti aggregati interessati, se presenti, nei casi di problematiche riguardanti i Servizi al cittadino offerti da questi ultimi sui Sistemi dell'Ente;

- c) l'Ente offre assistenza agli enti aggregati interessati, se presenti, e, ove applicabile, alla Società, per le fasi di autenticazione ai Sistemi dell'Ente e per le problematiche inerenti i Sistemi dell'Ente stesso.

Ai fini dell'assistenza sui Servizi al cittadino offerti tramite i Sistemi dell'Ente, l'Ente comunica alla Società, se del caso indicando appositi Delegati:

- a) un canale di contatto di tipo amministrativo per ciascun Servizio al cittadino di ciascun ente aggregato, se presente, specificando l'ufficio o il dipartimento competente a ricevere le richieste degli Utenti con riferimento all'erogazione del Servizio, da esporre in ciascuna Scheda Servizio;
- b) un canale di contatto di tipo tecnico deputato a ricevere le segnalazioni sul funzionamento dei Sistemi dell'Ente, che provengono dalla Società (anche su segnalazione degli Utenti), e dagli eventuali enti aggregati (anche tramite il contatto amministrativo di cui alla lett. a).

Gli eventuali ulteriori livelli di servizio, le previsioni in materia di incident response, escalation, service disruption e recovery delle informazioni con riferimento ai Sistemi dell'Ente saranno concordati tra le Parti tramite patti aggiuntivi che formeranno parte integrante dei presenti Termini Aggiuntivi. In assenza di specifici patti aggiuntivi, restano applicabili esclusivamente le previsioni dell'Accordo e del presente Addendum, senza che possano ritenersi assunti obblighi ulteriori e diversi.

Resta inteso, in ogni caso, che l'Ente si impegna a comunicare preventivamente alla Società le interruzioni programmate dei Sistemi dell'Ente, e tempestivamente le interruzioni straordinarie.

La Società accetta e riconosce che l'Ente potrebbe erogare Servizi al cittadino che hanno caratteristiche tali da poter interagire con software di terze parti pubbliche o private. A tal fine l'Ente garantisce alla Società di avere il diritto di utilizzare tali software per le finalità di cui all'Accordo e per tutta la durata dello stesso, impegnandosi a manlevare e tenere indenne la Società rispetto a qualsiasi malfunzionamento del software di terze parti nonché rispetto a qualsiasi pretesa avanzata da tali terze parti e/o dagli Utenti. Resta inteso, inoltre, che la Società non assume alcun obbligo di verifica circa la legittimità della licenze o il rispetto dei termini imposti dalle terze parti.

La Società accetta e riconosce, altresì, che ai software di terze parti potrebbero applicarsi termini e condizioni specifiche imposti da dette terze parti stesse, che potranno essere messi a disposizione della Società su richiesta di quest'ultima.

L'Ente resta responsabile dell'operato dei propri fornitori e sub-fornitori coinvolti nell'erogazione dei servizi accessibili tramite SSO, anche ai fini della protezione dei dati personali.

5. TRATTAMENTO DEI DATI PERSONALI

Le Parti agiscono in qualità di titolari autonomi del trattamento dei dati personali. Il Gestore è titolare del trattamento per l'identificazione su IO e la generazione dell'ID Token;

L'Ente Erogatore è Titolare autonomo per i trattamenti effettuati nell'erogazione del proprio servizio a valle dell'accesso.

La comunicazione dei dati tra le Parti è soggetta al consenso dell'Utente. L'Ente Erogatore si impegna a richiedere, tramite la configurazione del servizio sul Portale Back-office, esclusivamente il set minimo di attributi (claims) strettamente necessari all'erogazione del servizio, nel rispetto del principio di minimizzazione.

Il Gestore garantisce che l'Utente sia informato e, ove necessario, presti il consenso alla trasmissione dei propri dati all'Ente Erogatore prima del reindirizzamento. L'Ente Erogatore resta responsabile di fornire all'Utente la propria informativa privacy relativa al trattamento dei dati nell'ambito del servizio specifico erogato.

L'Ente Erogatore è responsabile di effettuare la propria analisi dei rischi e, qualora sussistano le condizioni di cui all'art. 35 del GDPR, la relativa Valutazione d'Impatto sulla Protezione dei Dati (DPIA) in merito ai trattamenti di propria competenza derivanti dall'utilizzo di SSO.

Le Parti si impegnano a informarsi reciprocamente e tempestivamente di qualsiasi minaccia o violazione che comporti rischi per gli interessati, provvedendo, autonomamente, per quanto di propria competenza, alle notifiche al Garante Privacy e alle comunicazioni agli interessati ex artt. 33 e 34 GDPR.

6. LICENZE, PROPRIETÀ INTELLETTUALE E RIUTILIZZO DELLA FUNZIONALITÀ

La Società è l'unica titolare di tutti i diritti, compresi i diritti di proprietà intellettuale e industriale, e i conseguenti diritti di utilizzazione economica, sulle soluzioni sviluppate per consentire la Funzionalità e l'integrazione tecnologica di cui ai presenti Termini Aggiuntivi, compreso il software e i kit (e.g. SDK) utilizzati per sviluppare l'integrazione stessa, inclusi in ogni caso i codici, gli elementi grafici e verbali che li compongono, e l'Ente accetta e riconosce che la Funzionalità e l'integrazione, compresa qualunque personalizzazione grafica e/o tecnica, potranno liberamente essere riutilizzate dalla Società, e la Società potrà sviluppare per soggetti terzi pubblici o privati personalizzazioni e integrazioni simili a, o basate su, le personalizzazioni e l'integrazione realizzate ai sensi dei presenti Termini Aggiuntivi, nonché fornire a soggetti terzi pubblici o privati servizi simili a, o basati su, le attività erogate ai sensi dei presenti Termini Aggiuntivi, senza che l'Ente abbia nulla a pretendere dalla Società, per qualsiasi titolo, ragione o causa.

L'Ente conserva i diritti preesistenti relativi ai Sistemi dell'Ente, alle soluzioni autonomamente sviluppate per consentire l'integrazione tecnologica di cui ai presenti Termini Aggiuntivi, e agli elementi contenuti nei materiali eventualmente forniti alla Società.

Ogni altra licenza, inclusi i termini e condizioni d'uso della Piattaforma IO e la disciplina relativa ai marchi e ai segni distintivi della Società e dell'Ente, resta regolata dalle previsioni dell'Accordo.

7. MODIFICHE E AGGIORNAMENTI DEI TERMINI AGGIUNTIVI E DELLA

DOCUMENTAZIONE TECNICA

Fermo restando quanto previsto all'art. 10 dell'Accordo, le Parti convengono sin da ora che i presenti Termini Aggiuntivi, potranno essere oggetto di modifica e aggiornamento nel tempo, anche in funzione dell'evolversi delle esigenze delle Parti, della normativa di riferimento e della tecnologia disponibile. Le Parti convengono pertanto che i relativi aggiornamenti e modifiche potranno essere portati a conoscenza dell'altra Parte anche tramite semplice pubblicazione sul Sito.

8. RISOLUZIONE E SOSPENSIONE DELLA FUNZIONALITÀ SSO

In caso di utilizzo non conforme di SSO o di rischi per la sicurezza o la protezione dei dati, PagoPA S.p.A. potrà sospendere o disabilitare l'accesso alla funzionalità per i servizi interessati, previa comunicazione all'Ente.

Qualora la Società accerti un grave inadempimento dell'Ente rispetto ad una delle obbligazioni di cui ai presenti Termini Aggiuntivi, la Società potrà intimare all'Ente, a mezzo PEC, di adempiere entro un congruo termine comunque non inferiore a 15 (quindici) giorni, con espressa avvertenza che decorso inutilmente detto termine, l'Accordo si intenderà senz'altro risolto ai sensi e per gli effetti di cui all'art. 1454 c.c., salvo il risarcimento del danno.

In caso di inadempimento, anche solo parziale o temporaneo, di una qualsiasi delle obbligazioni, dichiarazioni e garanzie dell'Ente previste dagli articoli 3 e 4, in quanto applicabili, dei presenti Termini Aggiuntivi, la Società avrà la facoltà di risolvere l'Accordo ai sensi e per gli effetti cui all'art. 1456 c.c., dandone comunicazione all'Ente e senza pregiudizio delle altre ipotesi di risoluzione e dei rimedi previsti da altre disposizioni dell'Accordo o dalla normativa applicabile.