AGID Agenzia per l'Italia Digitale

Linee guida recanti le regole tecniche dei gestori di attributi qualificati

Versione 1 del 18 luglio 2022

Versione	Determinazione di adozione	Tipologia modifica
1	DT 215/18.7.2022	Prima emissione

Sommario

Capitolo 1 Introduzione **4**
1.1 Scopo 4
1.2 Struttura 4
1.3 Gruppo di lavoro 5
1.4 Soggetti destinatari 5
Capitolo 2 Sigle e Riferimenti **6**
2.1 Principali riferimenti normativi 6
2.2 Standard di riferimento 6
2.3 Linee guida di principale riferimento 7
2.4 Termini e definizioni 7
2.5 Acronimi e abbreviazioni 8
Capitolo 3 Definizione d'insieme **10**
3.1. Accreditamento dei gestori di attributi qualificati 10
3.2 Attributi qualificati 11
3.3 Richieste di attributi qualificati 12
3.3.1 Richieste puntuali 13
3.3.2 Richieste continuative 13
3.4 Accesso e attestazione di attributi qualificati 14
Capitolo 4 Specifiche di funzionamento **15**
4.1 Flusso applicativo "public" 15
4.2 Flusso applicativo "protected" 16
4.3 Flusso applicativo "private" 17
4.4 Infrastruttura a chiave pubblica (pki) e trust model 18
4.5 Servizio di consultazione per l'utente 18
Capitolo 5 Protezione dei dati personali **20**

Capitolo 1
Introduzione

1.1 Scopo

La presente Linea guida (nel seguito LG) ha lo scopo di definire i requisiti per la realizzazione dell'architettura dei gestori di attributi qualificati (nel seguito anche Attribute Authorities) ai sensi dell'art. 1, comma 1, lettera m) del decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*" (nel seguito DPCM SPID).

La presente LG è emessa ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante "Codice dell'Amministrazione Digitale" (di seguito CAD) e della Determinazione AgID n. 160 del 2018 recante "*Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale*".

1.2 Struttura

Parte integrante della presente LG è l'allegato tecnico che definisce le specifiche tecniche implementative che possono variare nel tempo ma che non modificano il riferimento e le regole definiti nella presente LG:

- Allegato tecnico OAS3.

Ogni gestore di attributi qualificati ha la facoltà di definire in apposita documentazione le caratteristiche del servizio prestato, sempre nel rispetto delle presenti LG.

1.3 Gruppo di lavoro

La redazione del presente documento è stata curata da AgID con la collaborazione degli uffici di staff del Ministro per l'innovazione tecnologica e la transizione digitale.

1.4 Soggetti destinatari

I soggetti destinatari delle presenti LG sono tutti i soggetti coinvolti nella federazione SPID, con primario e principale focus sui gestori di attributi qualificati.

Nel rispetto delle presenti LG, la fruizione del servizio reso dai gestori di attributi qualificati è permesso anche ai soggetti presenti nella federazione CIE.

Capitolo 2

Sigle e Riferimenti

2.1 Principali riferimenti normativi

Sono riportati di seguito gli atti normativi di primario riferimento per il presente documento.

[CAD] Decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante "*Codice dell'amministrazione digitale*";

[DPCM SPID] Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID a parte delle pubbliche amministrazioni e delle imprese*";

[Regolamento eIDAS] Regolamento (UE) 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;

[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.

2.2 Standard di riferimento

Sono riportati di seguito gli standard tecnici di riferimento per l'applicazione del presente documento.

[OAS v3] Open API Specification v3

[RFC-7515] JSON Web Signature (JWS)

[SAMLcore] Security Assertion Markup Language (SAML) v2.0

2.3 Linee guida di principale riferimento

Di seguito sono elencate le Linee Guida e le Regole Tecniche emesse dall'AGID che verranno richiamate nel presente documento:

- Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni e Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici (Determinazione AgID n. 547/2021);
- Linee guida OpenID Connect in SPID (Determinazione AgID n. 616/2021);
- Linee guida contenenti le Regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD (Determinazione AgID n. 157/2020).

2.4 Termini e definizioni

Ai fini delle presenti Linee guida si applicano le definizioni di cui all'articolo 1 del CAD e si intende per:

- **Gestori di attributi qualificati**: ai sensi dell'art. 1, comma 1, lett. m) del DPCM SPID, sono "*i soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi*";
- **Attributi qualificati**: ai sensi dell'art. 1, comma 1, lett. e) del DPCM SPID, sono "*le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati*". L'art. 64, comma 2-duodecies, ultimo periodo del CAD - come da ultimo modificato dal D.L. 30 aprile 2022, n. 36, convertito, con modificazioni, dalla L. 29 giugno 2022, n. 79 - concorre a chiarire tale definizione, specificando che "*L'identità digitale, verificata ai sensi del presente articolo e con livello di sicurezza almeno significativo, attesta gli attributi qualificati dell'utente, ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, ovvero gli altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati, secondo le modalità stabilite da AgID con Linee guida*";

- **Richiesta di autenticazione**: l'evidenza informatica con la quale un SP richiede l'avvio di una sessione di autenticazione presso un IdP (nei contesti SAML e OIDC, si tratta della "*authentication request*");
- **Risposta di autenticazione**: l'evidenza informatica con la quale un IdP comunica a un SP i dati personali dell'interessato o il diniego a fornirli (nel contesto SAML, si tratta della "*response*"; nel contesto OIDC, si tratta della "*user-info*" o "*id token*");
- **Richiesta di attributi**: l'evidenza informatica con la quale un SP richiede a un'AA uno o più attributi qualificati di un soggetto;
- **Attestazione di attributi**: l'evidenza informatica con la quale un'AA comunica a un SP uno o più attributi qualificati;
- **Risposta di attributi:** attestazione di attributi o il diniego a fornirli;
- **Registro SPID**: ai sensi dell'art. 1, comma 1, lett. s) del DPCM SPID, è il "*registro, tenuto dall'Agenzia, accessibile al pubblico, contenente l'elenco dei soggettiabilitati a operare in qualità di gestori dell'identità digitale, di gestori degli attributi qualificati e di fornitori di servizi*" (https://registry.spid.gov.it);
- **Soggetti aggregatori:** soggetti pubblici o privati, convenzionati con AgID, che aggregano fornitori di servizi, rendendo accessibili tramite SPID i servizi di questi.

2.5 Acronimi e abbreviazioni

Di seguito si riportano gli acronimi e le abbreviazioni che verranno utilizzati nelle presenti LG:

- **AgID:** Agenzia per l'Italia Digitale;
- **SPID:** il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese, di cui all'art. 64 del CAD;
- **PA**: Pubblica Amministrazione;
- **IdP**: identity provider, il gestore dell'identità digitale;
- **SP:** Service Provider, il fornitore di servizi;
- **AA**: attribute authority, il gestore di attributi qualificati;
- **AGGR**: Soggetti aggregatori;
- **CA**: certificate authority;
- **OAS3**: OpenAPI Specification (OAS), versione 3.0;

- **CIE:** Carta di Identità Elettronica;
- **JSON**: JavaScript Object Notation, come previsto dalla norma RFC-8259;
- **JWT:** pacchetto JSON (JSON Web Token), come previsto dalla norma RFC-7797;
- **JWE:** JWT cifrato, come previsto dalla norma RFC-7516;
- **JWS:** JWT firmato, come previsto dalla norma RFC-7515;
- **OIDC:** standard OpenID Connect pubblicato da OpenID® Foundation;
- **IPA:** l'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubbliciservizi
- **PKI:** Public Key Infrastructure (infrastruttura a chiave pubblica), basata su certificati elettronici conformi a RFC-5280;
- **QTSP:** prestatore di servizi fiduciari qualificati ai sensi del Regolamento eIDAS;
- **QSEAL:** sigillo elettronico avanzato, come da Regolamento eIDAS;
- **SAML:** standard Security Assertion Markup Language, versione 2.0, pubblicato da OASIS.

Capitolo 3
Definizione d'insieme

3.1. Accreditamento dei gestori di attributi qualificati

Ai sensi dell'art. 1, comma 1, lett. m) del DPCM SPID, le AA si collocano fra i soggetti operanti nella federazione SPID.

Può accreditarsi quale AA qualunque soggetto che si collochi, in base alle norme vigenti, nell'alveo della definizione formulata all'art. 1, comma 1, lett. m) del DPCM SPID, come specificata nella presenti LG al precedente paragrafo 2.4.

L'art. 16 del DPCM SPID disciplina l'accreditamento delle AA, stabilendo al comma 1 che "*[…] si accreditano indicando i dati che intendono rendere disponibili nello SPID, nel rispetto del presente decreto e secondo le modalità indicate nei regolamenti attuativi adottati ai sensi dell'art. 4*".

Ai sensi dell'articolo 4, lettere a) e c) del DPCM SPID, le AA stipulano una apposita Convenzione con l'AgID al fine di operare all'interno della federazione SPID.

Ai sensi dell'art. 16, comma 2 del DPCM SPID, l'AgID inserisce nel Registro SPID - accessibile da parte dei fornitori di servizi - le tipologie di dati resi disponibili da ciascuna AA. Presso il registro SPID, pertanto, è pubblicato un registro delle AA e a queste è reso disponibile il relativo documento OpenAPI.

A norma del comma 3 del citato art. 16 del DPCM SPID, sono infine individuati i soggetti che, a fronte di relativa richiesta, sono accreditati di diritto quali AA:

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

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

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

d) l'AgID in relazione ai dati contenuti nell'IPA di cui all'articolo 6-ter del CAD.

3.2 Attributi qualificati

L'attributo qualificato - la cui definizione ai sensi delle presenti LG è formulata al precedente paragrafo 2.4, ai sensi dell'art. 1, comma 1, lett. e) del DPCM SPID e dell'art. 64, comma 2-duodecies, ultimo periodo del CAD - è richiesto dal SP ai soli fini della fruizione di uno specifico servizio a cui l'interessato intende accedere.

L'individuazione, la descrizione e la modalità di messa a disposizione degli attributi qualificati che l'AA è in grado di attestare è demandata alla stessa AA che li rende disponibili, nel rispetto della protezione dei dati sin dalla progettazione e per impostazione predefinita ai sensi dell'art. 25 del GDPR e della responsabilizzazione dell'AA ai sensi dell'art. 5, par. 2 del GDPR.

Si specifica che le AA devono assicurare, per impostazione predefinita, il trattamento dei soli dati personali necessari per ogni specifica finalità del trattamento, tenendo conto dell'effettivo contenuto informativo da fornire ai SP e ciò, ad esempio, privilegiando attributi di tipo booleano o comunque fornendo le informazioni minime necessarie per attestare il possesso dell'attributo richiesto, nel rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. C) del GDPR.

Tali cautele vanno apprestate, a maggior ragione e con particolare rigore, nei casi in cui il trattamento riguardi attributi qualificati appartenenti alle categorie particolari di cui all'art. 9 del GDPR o concernenti dati relativi a condanne penali e reati di cui all'art. 10 del GDPR, i quali:

- possono essere richiesti esclusivamente per la fruizione di servizi non possono essere erogati senza la conoscenza di tali attributi dell'utente (ad esempio: assenza di condanne penali per la partecipazione a un concorso pubblico o l'iscrizione in un albo professionale);

- possono essere resi conoscibili unicamente dalle AA che sono espressamente e specificamente individuate dall'ordinamento come i soggetti abilitati all'attestazione di tali categorie di attributi (ad esempio: con riferimento all'esemplificazione di cui al punto precedente, l'attributo

qualificato dell'assenza o presenza di condanne penali a carico del candidato a un concorso pubblico potrà essere attestato unicamente dal Ministero della Giustizia mediante il Casellario giudiziale);

- comportano il dovere, in capo al SP che riceve tali attributi qualificati per consentire la fruizione di un servizio, della necessaria messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 32 del GDPR.

3.3 Richieste di attributi qualificati

Qualora sia necessario conoscere un attributo qualificato del soggetto interessato ai fini dell'erogazione di un determinato servizio online, il SP informa di tale necessità l'utente che intende accedere al servizio, indicando, per ogni attributo qualificato, anche l'AA presso cui sarà richiesto.

Per l'ottenimento di uno o più attributi qualificati, il SP (anche per il tramite di un AGGR) invia una richiesta di attributi a una o più AA.

Qualora gli attributi qualificati siano attestabili dalla medesima AA, il SP invia a tale AA un'unica richiesta di attributi, a meno che alcuni di questi siano soggetti a dipendenze verificabili solo previa attestazione di altri attributi qualificati.

Al fine di dar utilmente seguito alle richieste di attributi, l'AA definisce, nelle proprie specifiche OAS3 conformi alle citate Linee guida in materia di interoperabilità, gli elementi obbligatori che i SP devono necessariamente inserire nelle richieste.

Ogni richiesta di attributi qualificati, indirizzata a un'AA da parte di un SP, si caratterizza per:

a) l'identificazione del soggetto a cui i riferiscono gli attributi;
b) la caratteristica temporale della richiesta: puntuale o continuativa.

3.3.1 Richieste puntuali

La richiesta è puntuale quando è volta a ottenere un'unica e immediata attestazione da parte dell'AA.

3.3.2 Richieste continuative

La richiesta è continuativa quando è volta a ottenere, da parte dell'AA, più attestazioni "asincrone" del/i medesimo/i attributo/i qualificato/i all'interno di una finestra temporale - non superiore a un periodo ininterrotto di 12 mesi - reciprocamente concordata tra SP, AA e utente.

Si evidenzia che il SP deve sempre effettuare un'autonoma, motivata e dimostrabile valutazione in merito alla necessità di eseguire una richiesta continuativa di attributi qualificati per la specifica finalità del servizio.

Si chiarisce, tuttavia, che il SP può usufruire di tale tipoligia di richiesta solo se l'AA destinataria offre effettivamente tale possibilità.

Nello specifico, il SP propone all'AA una richiesta continuativa di attributi qualificati costituita, dal punto di vista informatico, da un'autorizzazione di lunga durata. Ricevuta la richiesta, l'AA valuta se ammettere la richiesta continuativa e, qualora l'esito di tale valutazione sia positivo, valuta altresì se il periodo temporale proposto dal SP è accettabile o eccessivo, abbreviando se del caso la finestra temporale dell'autorizzazione proposta dal SP.

Nel caso in cui la richiesta continuativa sia valutata come accettabile dall'AA, anche mediante eventuale riduzione del periodo temporale, questa è tenuta a richiedere all'utente un assenso esplicito (che interviene mediante autenticazione dell'utente interessato anche presso l'AA mediante il proprio IdP) prima di procedere all'attestazione degli attributi richiesti e previa informativa sul trattamento dei suoi dati personali.

L'utente, a sua volta, può decidere se:

a) negare l'assenso alla richiesta continuativa;
b) convertire la richiesta continuativa in una richiesta puntuale;
c) ridurre ulteriormente la durata temporale a un periodo inferiore di propria scelta.

Ricevuta dall'AA una risposta positiva alla richiesta inoltrata, il SP può inviare all'AA, durante il periodo temporale concordato, richieste asincrone degli indicati attributi qualificati,

senza che intervenga alcun ulteriore processo di autenticazione né un ulteriore assenso esplicito da parte dell'utente.

All'approssimarsi della scadenza del periodo concordato, il SP può chiedere all'utente il rinnovo o l'estensione di tale periodo per un massimo di ulteriori 12 mesi continuativi, qualora ne valuti la necessità ai fini della fruizione del servizio reso.

3.4 Accesso e attestazione di attributi qualificati

Come meglio specificato nell'Allegato alle presenti LG, l'accesso agli attributi e, di conseguenza, la loro attestazione possono essere classificati sulla base delle seguenti casistiche:

a) "**public**": il dato è open, di pubblico dominio o liberamente accessibile. In tal caso l'accesso al dato non richiede l'acquisizione dell'assenso dell'utente da parte dell'AA;

b) "**protected**": l'accesso al dato è riservato ai SP che hanno una specifica convenzione con l'AA. In tal caso, per l'accesso non è richiesta l'acquisizione dell'assenso dell'utente da parte dell'AA;

c) "**private**": l'accesso al dato è consentito solo previa acquisizione dell'assenso dell'utente da parte dell'AA. Tale casistica si applica sempre nei casi di richiesta continuativa di attributi qualificati.

I flussi di accesso e di attestazione degli attributi qualificati sono specificati nel capitolo seguente.

Capitolo 4

Specifiche di funzionamento

4.1 Flusso applicativo "public"

Il presente flusso si applica nei casi di accesso "public".

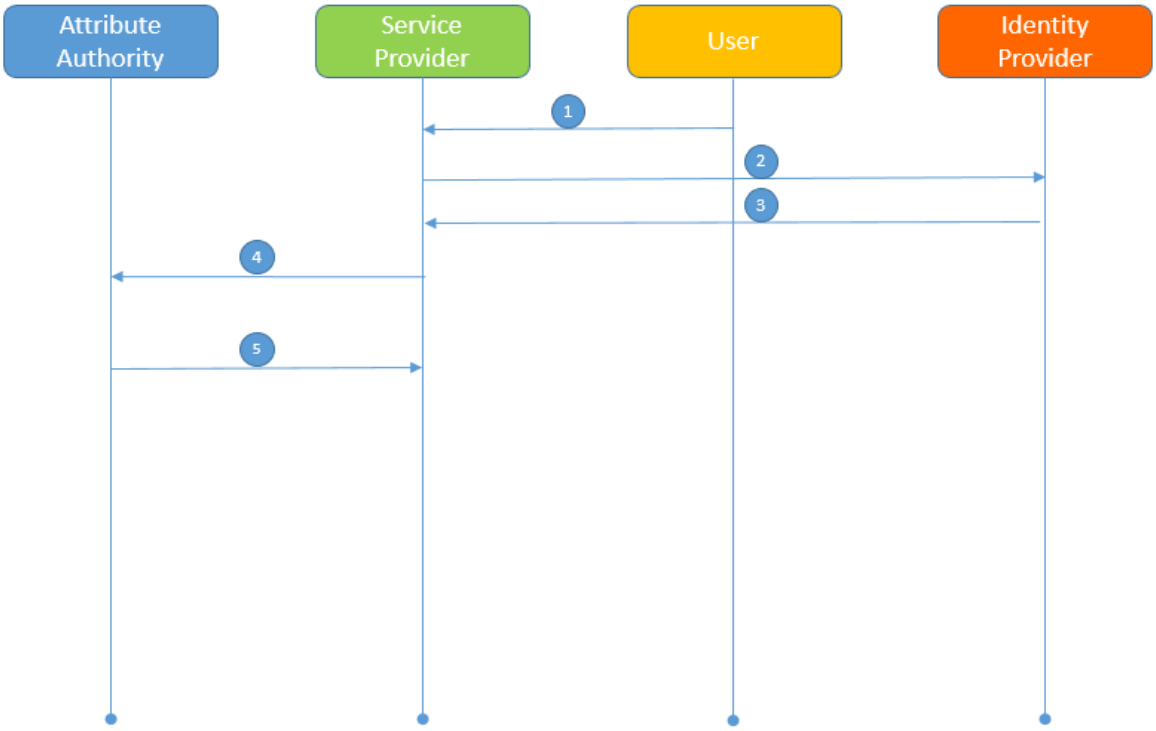

Figura 1- Flusso applicativo "public"

1. L'utente chiede l'accesso a un servizio del SP per la cui fruizione è necessaria l'acquisizione di uno o più attributi qualificati e seleziona l'IdP che gestisce la propria identità digitale.
2. Il SP, informato l'utente sul trattamento dei suoi dati personali, inoltra quest'ultimo presso l'IdP.
3. L'IdP esegue la procedura di autenticazione e invia la risposta di autenticazione al SP.
4. Il SP invia la richiesta all'AA.

5. L'AA riscontra direttamente il SP mediante attestazione degli attributi richiesti.

4.2 Flusso applicativo "protected"

Il presente flusso si applica nei casi di accesso "protected".

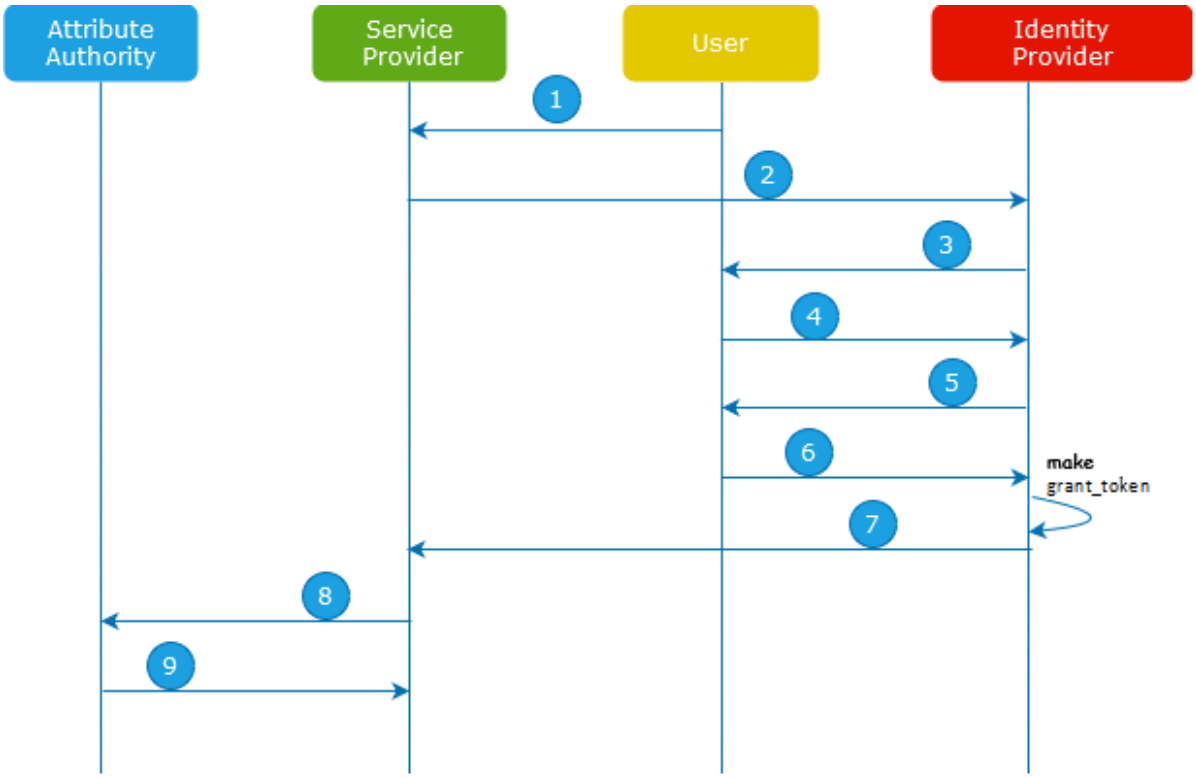

Figura 2 - Flusso applicativo "protected"

1. L'utente chiede l'accesso a un servizio del SP per la cui fruizione è necessaria l'acquisizione di uno o più attributi qualificati e seleziona l'IdP che gestisce la propria identità digitale.
2. Il SP, informato l'utente sul trattamento dei suoi dati personali, inoltra quest'ultimo presso l'IdP e, nella richiesta di autorizzazione, dichiara le AA che potrebbe potenzialmente interrogare ai fini dell'erogazione dei servizi resi.
3. L'IdP, nell'eseguire la procedura di autenticazione, mostra all'utente le AA indicate dal SP.
4. L'utente seleziona le AA per la cui interrogazione vuole fornire l'assenso al SP.
5. L'IdP, durante la medesima procedura di autenticazione, chiede all'utente l'assenso alla trasmissione dei propri dati al SP e all'interrogazione da parte del SP delle AA selezionate.

6. L'utente rende il proprio assenso.
7. L'IdP genera un token di concessione (grant_token) per ognuna delle AA selezionate, reindirizza l'utente sul SP con la risposta (response) contenente il token di concessione.
8. Il SP invia il token di concessione (grant_token) alla/e AA.
9. L'AA, sulla base del token di concessione (grant_token) e dei controlli specifici derivanti dalla Convenzione stipulata dal SP, fornisce a quest'ultimo un'autorizzazione per recuperare gli attributi qualificati.

Tale flusso è maggiormente dettagliato nell'Allegato tecnico alle presenti LG.

4.3 Flusso applicativo "private"

Il presente flusso si applica nei casi di accesso "private".

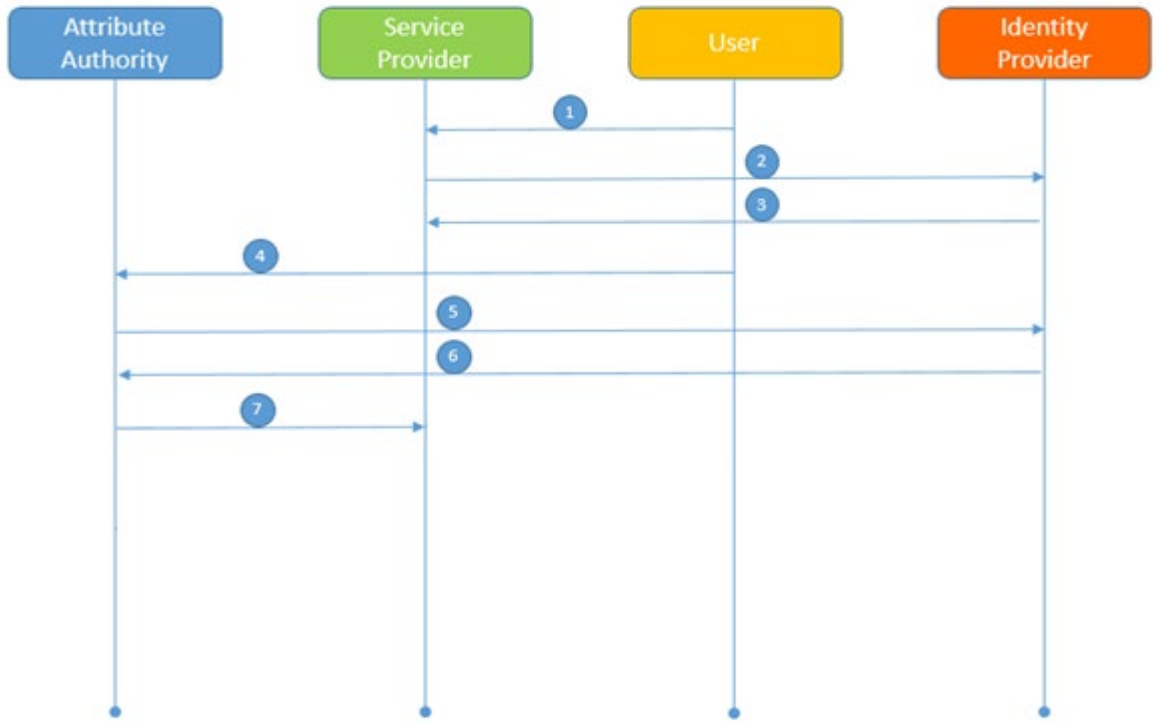

Figura 3 - Flusso applicativo "private"

1. L'utente chiede l'accesso a un servizio del SP per la cui fruizione è necessaria l'acquisizione di uno o più attributi qualificati e seleziona l'IdP che gestisce la propria identità digitale.

2. Il SP, informato l'utente sul trattamento dei suoi dati personali, inoltra quest'ultimo presso l'IdP.
3. L'IdP esegue la procedura di autenticazione e invia la risposta di autenticazione al SP.
4. Il SP invia all'AA la richiesta di attributi qualificati dell'utente, reinoltrando quest'ultimo presso l'AA stessa.
5. L'AA, informato l'utente sul trattamento dei suoi dati personali, lo inoltra presso l'IdP per l'autenticazione.
6. L'IdP esegue la procedura di autenticazione e invia la risposta di autenticazione all'AA.
7. L'AA fornisce al SP un'autorizzazione per recuperare gli attributi qualificati; il SP invia la richiesta all'AA per recuperare gli attributi qualificati; l'AA riscontra direttamente il SP mediante attestazione degli attributi richiesti.

Tale flusso è maggiormente dettagliato nell'Allegato tecnico alle presenti LG.

4.4 Infrastruttura a chiave pubblica (pki) e trust model

È istituita presso AgID un'infrastruttura a chiave pubblica (PKI) gerarchica, mediante una CA radice (root CA). Tramite tale sistema di fiducia, AA e SP possono verificare la firma dei messaggi scambiati con altri attori della federazione.

4.5 Servizio di consultazione per l'utente

Nel caso in cui sia previsto per norma e/o nel caso in cui siano consentite richieste di attributi continuative per mezzo di autorizzazioni di lunga durata, l'AA deve rendere disponibile all'utente di un servizio di consultazione, accedibile tramite gli strumenti previsti all'art. 64 del CAD, ove può prendere visione delle trasmissioni dei propri attributi qualificati inviati ai SP.

Nel caso in cui, invece, il servizio di consultazione non sia previsto per norma e/o l'AA non accetti richieste continuative, l'implementazione del servizio di consultazione per l'utente è facoltativa.

Nel primo caso, l'utente può usare servizi di consultazione per:

- verificare a quali SP sono stati trasmessi gli attributi o è stato concesso il loro trasferimento periodico;
- verificare la data, l'ora e l'attestazione di attributi inviata per ciascuna delle richieste continuative intervenute nel periodo concordato nell'autorizzazione di lunga durata;
- accorciare la durata dell'autorizzazione di lunga durata;
- revocare l'autorizzazione di lunga durata.

Il servizio di consultazione deve essere implementato come API OAS3 ed essere esposto all'utente tramite applicazione web mobile.

Capitolo 5

Protezione dei dati personali

Con specifico riferimento ai flussi descritti nelle presenti LG, si ritiene essenziale chiarire che l'assenso dell'interessato non costituisce la base giuridica di cui all'art. 6, par. 1, lett. a) del GDPR, rappresentando la mera conferma circa l'effettiva conoscenza degli attributi qualificati che saranno trattati e dei soggetti che li tratteranno. Tale conferma interviene durante la procedura di autenticazione dell'interessato ad opera dell'IdP, così come avviene per i dati personali che l'IdP dichiara di trasmettere al SP durante l'autenticazione dell'utente in ambito SPID.

Le AA agiscono nel rispetto della normativa unionale europea e nazionale in materia di protezione dei dati personali, avendo cura di valutare sempre - sin dalla progettazione e per impostazione predefinita - l'effettivo rispetto dei principi di cui all'art. 5 del GDPR.

Con riferimento alla richiesta di attributi qualificati, il SP è tenuto a valutare - sin dalla progettazione e per impostazione predefinita - l'effettiva necessità di acquisire tali attributi afferenti l'interessato per le finalità del servizio erogato e ad approntare il relativo trattamento nel rispetto scrupoloso dei principi di cui all'art. 5 del GDPR, con particolare riferimento ai principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati rispetto alle finalità individuate e limitazione della conservazione, essendo in grado di comprovare il rispetto di tali principi ai sensi dell'art. 5, par. 2 del GDPR.

Il SP è sempre tenuto a rendere all'interessato una chiara ed esaustiva informativa sul trattamento dei suoi dati personali, indicando anche gli attributi qualificati che necessita di chiedere all'AA per le finalità di fruizione del servizio in rete.

Con riferimento alla conservazione dei dati personali, le richieste e le relative attestazioni di attributi sono conservate per 24 mesi esclusivamente a fini probatori e nel rispetto di quanto prescritto nel decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché*

dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese" e nel "*Regolamento recante le modalità attuative per la realizzazione dello SPID*", adottato con Determinazione AgID n. 44 del 28 luglio 2015.

Nei trattamenti dei dati personali costituiti dagli attributi qualificati, IdP, SP e AA agiscono sempre quali titolari autonomi.

IdP, SP e AA sono tenuti ad adottare le misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, a 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, informandosi reciprocamente e tempestivamente in caso di violazioni di sicurezza o di qualsiasi minaccia, intervenute nei processi di cui alle presenti LG, che comportino un rischio per la sicurezza e per i diritti e le libertà degli interessati, anche al fine di agevolare l'adempimento degli obblighi di cui agli artt. 33 e 34 del GDPR.