Linee Guida Attribute Authority SPID

Release master

AGID

17 giu 2021

Indice dei contenuti

1 Introduzione **3**
- 1.1 Scopo . . . 3
- 1.2 Struttura . . . 3
- 1.3 Gruppo di lavoro . . . 3
- 1.4 Soggetti destinatari . . . 4

2 Sigle e Riferimenti **5**
- 2.1 Riferimenti Normativi . . . 5
- 2.2 Standard di riferimento . . . 5
- 2.3 Linee guida di riferimento . . . 5
- 2.4 Termini e definizioni . . . 6
- 2.5 Acronimi e abbreviazioni . . . 6
- 2.6 Basi giuridiche . . . 7

3 Descrizione d'insieme **9**
- 3.1 Attributi qualificati . . . 9
- 3.2 Convenzioni . . . 10
- 3.3 Attestazione di attributo . . . 10
- 3.4 Tipologie di richiesta . . . 11

4 Specifiche di funzionamento **13**
- 4.1 Flusso applicativo senza necessità del consenso dell'utente . . . 13
- 4.2 Flusso applicativo che richiede il consenso dell'utente . . . 14
- 4.3 Infrastruttura a chiave pubblica (pki) e trust model . . . 15
- 4.4 Servizio di consultazione per l'utente . . . 15
- 4.5 Registro delle Attribute Authority . . . 15

Linee Guida contenenti le

Regole tecniche dei gestori di attributi qualificati ex art.1, comma 1, lettera m) del DPCM 24 ottobre 2014 (GU n.285 del 9122014)

Versione 1.0 – maggio 2021

Versione	Data	Tipologia modifica
1.0	Maggio 2021	Prima emanazione

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

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

CAPITOLO 1

Introduzione

1.1 Scopo

La presente **Linea guida - Regola Tecnica,** nel seguito indicata come LG, ha lo scopo di definire i requisiti per la realizzazione dell'architettura dei gestori di attributi qualificati ex art.1, comma 1, lettera m) del DPCM 24 ottobre 2014 (GU n.285 del 9122014), nel seguito Attribute Authority.

La presente LG viene emessa ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (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 sono i seguenti allegati e tecnici che definiscono le specifiche tecniche implementative che possono variare nel tempo ma che non modificano il riferimento e le regole definite nella presente LG:

- Allegato tecnico OAS3
- Allegato tecnico SAML (riservato alla AA Gestore delle deleghe, amministrazioni di sostegno e tutele)

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 dal gruppo di lavoro AgID con la collaborazione del Ministero per l'Innovazione tecnologica e la la digitalizzazione.

1.4 Soggetti destinatari

I soggetti destinatari delle presenti LG sono i soggetti gestori di attributi qualificati, ovvero, potenzialmente, tutti i soggetti che in base ad una norma hanno il potere di attestare qualifiche, stati personali, poteri di persone fisiche.

CAPITOLO 2

Sigle e Riferimenti

2.1 Riferimenti Normativi

Sono riportati di seguito gli atti normativi di riferimento del presente documento.

- **[D.Lgs. 82/2005]** Decreto legislativo 7 marzo 2005, n. 82 recante "Codice dell'amministrazione digitale"; NOTA – Il D. Lgs. 82/2010 è noto anche con l'abbreviazione "CAD"

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 riferimento

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

- Linea di indirizzo sulla interoperabilità tecnica (Determinazione AgID n. 406/2020);
- Linee guida contenenti Regole tecniche relative all'uso di OpenID® Connect nella federazione SPID;
- Linee guida contenenti Regole tecniche circa la sottoscrizione elettronica di documenti mediante SPID ex art. 20 del CAD.

2.4 Termini e definizioni

Ai fini delle presenti Linee guida, oltre ad applicarsi le definizioni di cui all'articolo 1 del CAD, si intende per:

- **Attestazione di attributo/i** : cfr. 'risposta di attributi';
- **Attributi qualificati** : le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati, ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualita" personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, secondo le modalita" stabilite da AgID con Linee guida.
- **Gestori di attributi qualificati**: i soggetti accreditati ai sensi dell'art. 16 del DPCM 24 0ttobre 2014 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi;
- **Registro SPID** : elenco dei soggetti appartenenti alla federazione SPID, disponibile su internet all'indirizzo https://registry.spid.gov.it che pubblica, per ciascuno di essi, le informazioni pubbliche di pertinenza per lo schema, come ad esempio il codice IPA e il campo entityId;
- **Regolamento eIDAS** : 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;
- **Regolamento GDPR** : Regolamento (UE) N°679/2016 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;
- **Richiesta di autenticazione** : l'evidenza informatica con la quale un SP richiede l'avvio di una sessione di autenticazione presso un IDP (cioè l'authentication request nei contesti SAML e OIDC);
- **Richiesta di attributi** : l'evidenza informatica con la quale un SP richiede a un'AA uno o più attributi qualificati di un soggetto;
- **Risposta di autenticazione** : l'evidenza informatica con la quale un IDP comunica i dati personali, o il diniego a fornirli, presso un SP (response nel contesto SAML; user-info o id token nel contesto OIDC);
- **Risposta di attributi** : l'evidenza informatica con la quale un'AA comunica a un SP uno o più attributi qualificati (cd. attestazione di attributo), ovvero il diniego a fornirli;

2.5 Acronimi e abbreviazioni

Di seguito si riportano gli acronimi e le abbreviazioni che verranno utilizzati nella presente Linee Guida:

- **Agenzia** o **AgID :** Agenzia per l'Italia Digitale;
- **PA** : Pubblica Amministrazione;
- **AA** : attribute authority (gestori di attributi qualificati);
- **CA** : certificate authority;
- **CAD** : D.Lgs. 7 marzo 2005 N°82, Codice dell'Amministrazione Digitale, e s.m.i.
- **OIDC** : OpenID Connect;
- **OAS3** : OpenAPI Specification (OAS), versione 3.0;
- **CF** : codice fiscale;
- **CIE** : Carta di Identità Elettronica;
- **IDP** : identity provider;

- **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;
- **OAS3** : si veda OpenAPI;
- **OIDC** : standard OpenID Connect pubblicato da OpenID® Foundation;
- **IPA** : indice degli indirizzi della pubblica amministrazione;
- **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;
- **SP** : fornitore di servizi nella federazione SPID, ovvero service provider nel contesto SAML, ovvero relying party nel contesto OIDC;
- **SPID** : Sistema Pubblico di Identità Digitale, introdotto con il DPCM del 24 ottobre 2014, articolo 4, comma 2 e successive modificazioni;

2.6 Basi giuridiche

L'articolo 1, comma 1, lett. m), decreto del Presidente del Consiglio dei ministri 24 ottobre 2014 definisce i gestori di attributi qualificati (AA) come:

[...] i soggetti accreditati ai sensi dell'articolo 16 che hanno il potere, in base alle norme vigenti, di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.

Tali attributi qualificati sono definiti, all'articolo 1, comma 1, lett. e), decreto del Presidente del Consiglio dei ministri 24 ottobre 2014, come:

[...] le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.

L'articolo 16, comma 3, prevede che:

Su richiesta degli interessati, sono accreditati di diritto i seguenti gestori di attributi qualificati:

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'Agenzia in relazione ai dati contenuti nell'indice degli indirizzi della pubblica amministrazione (IPA) e dei gestori di pubblici servizi di cui all'articolo 6-ter del CAD.

L'articolo 64 del CAD, come modificato dal decreto semplificazioni, garantisce il diritto dei cittadini di accedere ai servizi online con lo SPID e con la CIE. Pertanto, la fruizione dei servizi derivanti dalle seguenti linee guida devono essere garantiti anche ai cittadini che utlizzano la CIE (in seguito, federazione CIE) per l'accesso ai servizi in rete.

CAPITOLO 3

Descrizione d'insieme

3.1 Attributi qualificati

Un attributo qualificato descrive una proprietà di un'identità. Esso si definisce qualificato perché è attestato da soggetto cui la legge conferisce tale potere. Di solito gli attributi qualificati non cambiano frequentemente nel tempo, e il numero di operazioni in lettura è molto maggiore di quelle in scrittura; ad esempio, l'attributo associato ad una patente di guida cambierà alla scadenza del documento, ma nel frattempo verrà letto numerose volte.

All'interno delle federazioni SPID e CIE possono sussistere diverse tipologie di attributi qualificati, dipendenti dalla specifica AA che accede al circuito mediante stipula di una convenzione. La descrizione di tali attributi è, pertanto, demandata alla specifica AA. Può accreditarsi come AA, qualunque soggetto che ha il potere di attestare il possesso e la validità di attributi qualificati in base alle norme vigenti.

La seguente tabella mostra alcuni esempi di possibili AA e i relativi attributi qualificati.

Entità	Attributi	Esempi di servizi abilitati
ASL /SSN / Fascicolo Sanitario	status invalido civile	Richiesta permesso ZTL
Catasto	Immobili intestati; rendite immobiliari	Precompilazione campi per domande (ad es. TARI)
Gestore delle deleghe, amministrazioni di sostegno e tutele	Deleghe e procure digitali	Attributi identificativi del delegante che ha creato una delega digitale: per tutti i servizi di un SP; per una specifica classe di servizi di un SP; per una specifica operazione appartenente ad una classe di servizi di un SP. Informazioni afferenti la delega.
IndicePA*	Amministrazione di appartenenza; ruolo	Servizi riservati a dipendenti pubblici
INPS	ISEE; status pensionistico	Accesso a servizi con policy basate sull'ISEE
Ministero dell'Interno (ANPR)	Stato civile; familiari; luogo di residenza; lista elettorale; titolo di studio e tutti gli altri campi previsti dal DPCM 194/2014	Richiesta permesso ZTL; accesso a servizi comunali/regionali
Motorizzazione	Classe patente; neopatentato; saldo punti patente	
Notariato*	Appartenenza al Notariato	Servizi riservati a notai
Ordini professionali*	Appartenenza ad un ordine	Servizi riservati a professionisti (concorsi ecc.)
Pubblico Registro Automobilistico	Veicoli intestati	
Registro delle Imprese*[2]	Imprese di cui il soggetto è socio o detiene cariche	Servizi alle imprese; verifica dei poteri di rappresentanza; deleghe
Registro INIPEC*	PEC	

3.2 Convenzioni

I Gestori di attributi qualificati (AA) ai sensi dell'articolo 4 lettera c) del DPCM 26 ottobre 2014, stipulano apposita Convenzione con l'Agenzia.

3.3 Attestazione di attributo

Le attestazioni di attributo prodotte da un'AA servono ad attestare uno o più attributi qualificati riguardo ad una persona fisica o giuridica, previa richiesta da parte di un SP.

Per erogare un servizio, il SP può aver bisogno di una molteplicità di attributi qualificati attestabili da AA differenti; gli attributi qualificati attestabili dalla medesima AA sono preferibilmente raccolti in un'unica richiesta di attributi, a meno che alcuni di questi attributi siano soggetti a dipendenze verificabili solo previa attestazione di altri attributi qualificati

[2] previsti espressamente dal DPCM del 24 ottobre 2014

Le richieste e le risposte di attributi sono conservate per 24 mesi al fine di poter ricostruire, in caso di richiesta da parte di un interessato, il flusso dei dati personali ad esso riferiti. Fatte salve diverse disposizioni di carattere normativo o amministrativo, è fatto divieto alle AA e ai SP di conservare tali informazioni per un periodo di tempo superiore, nonché di trattare le predette informazioni per finalità diverse da quelle sopraindicate.

È fatto altresì divieto alle AA e ai SP di trattare ogni altro dato personale di cui siano venuti a conoscenza o a cui abbiano avuto accesso per le finalità indicate o in attuazione delle presenti linee guida, per finalità ultronee a quelle indicate nelle stesse.

3.4 Tipologie di richiesta

Le singole AA definiscono nelle proprie specifiche OAS3, conformi alle indicazioni delle LL.GG. Interoperabilità, emanate da Agid, quali siano gli elementi obbligatori che i SP devono inserire nelle richieste. Fermo restando l'uso esclusivo delle specifiche OAS3, esclusivamente per la AA che gestisce le deleghe, amministrazioni di sostegno e tutele, può, in prima istanza, essere utilizzata l'interfaccia SAML come normato nello specifico allegato delle presenti LG.

Ogni richiesta di attributi qualificati si caratterizza per:

a) identificazione del soggetto;

b) sincronicità della richiesta di attributi qualificati: puntuale o continuativa;

c) verifica della necessità di rilascio del consenso da parte dell'utente alla fornitura di attributi qualificati.

Le interrogazioni alle AA sono caratterizzate dalla tipologia dei dati richiesti, da cui discende l'obbligatorietà da parte delle AA di acquisire o meno il consenso dell'interessato alla comunicazione dei propri dati al richiedente (punto a). Per ottenere tale consenso può essere necessario che la stessa AA acquisisca il consenso dall'interessato. In altri casi, invece, è possibile che l'AA preveda che il consenso sia raccolto dal SP.

I SP possono richiedere dati personali nei casi previsti dalla norma con particolare riferimento al GDPR e al codice privacy.

Qualunque sia la tipologia di identificazione, l'AA decide se (punto c):

- gli attributi qualificati possono essere inviati al SP previo consenso acquisito dal SP o in assenza dello stesso consenso
- è necessario richiedere all' utente il consenso esplicito per l'invio dei dati al SP.

É prevista (punto b), la possibilità per il SP di richiedere gli attributi qualificati una tantum (richieste puntuali), o di effettuare più richieste dei medesimi attributi in automatico nell'arco di un periodo di lunga durata (richieste continuative).

Richieste puntuali

La richiesta di attributi qualificati è puntuale quando, se accolta, viene seguita da un'unica immediatamente "sincrona" risposta di attributi da parte dell'AA.

Richieste continuative

Le AA possono prevedere richieste continuative.

La richiesta di attributi qualificati è continuativa quando, se accolta, un SP indirizza ad una AA, relativamente agli stessi attributi qualificati iniziali, molteplici richieste "asincrone" di attributi, all'interno di una finestra temporale reciprocamente concordata tra SP, AA e utente. Tale finestra temporale non potrà in nessun caso essere superiore ad un periodo ininterrotto di 12 mesi.

La richiesta continuativa è costituita da un consenso di lunga durata, inizialmente proposto dal SP all'AA che, qualora il consenso sia accordato, valuta se ammetterne la continuità o meno. L'AA può ritenere la durata eccessiva e, nel caso, ridurre la finestra temporale a un periodo inferiore rispetto a quanto proposto dal SP.

Nel caso in cui il consenso di lunga durata sia ammissibile da parte dell'AA, quest'ultima richiede all'utente di accettare esplicitamente la finestra temporale, eventualmente abbreviata dall'AA. L'utente può decidere se:

a) negare tale richiesta continuativa (e quindi negare il consenso a fornire gli attributi qualificati in oggetto),

b) convertire la richiesta in una richiesta puntuale, oppure

c) ridurre ulteriormente la durata della finestra temporale a un qualunque periodo inferiore di propria scelta.

Una volta acquisito il consenso, il SP può inviare all'AA delle richieste asincrone limitatamente agli attributi per cui è stata autorizzata la trasmissione, durante il periodo concordato, senza che intervenga alcun ulteriore processo di autenticazione o autorizzazione da parte dell'utente.

All'approssimarsi della scadenza del periodo concordato l'AA può informare l'utente dell'opportunità di rinnovare o estendere tale periodo per ulteriori 12 mesi privi di interruzioni .

Il consenso di lunga durata può avere profonde implicazioni in merito alla minimizzazione dei dati personali. Per tale motivo è sempre richiesto nel rispetto di quanto previsto dai considerando 71, 78 e 156 e dall'articolo 5, comma 1,lett. c) del Regolamento GDPR.

CAPITOLO 4

Specifiche di funzionamento

4.1 Flusso applicativo senza necessità del consenso dell'utente

Tale flusso si applica anche nel caso in cui il consenso dell'utente sia già stato acquisito dal SP.

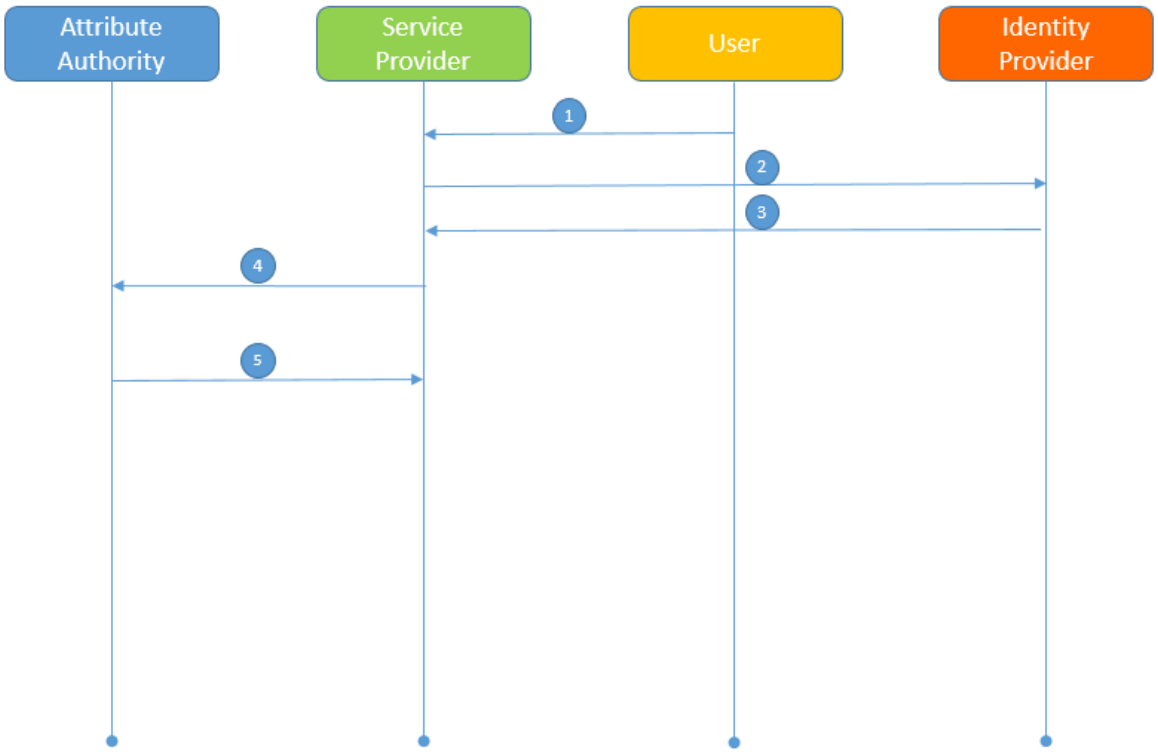

Figura 1 Flusso di richiesta di attributi qualificati senza consenso o consenso acquisito dal SP.

Nel caso di richiesta "sincrona" (cfr. Figura 1):

1. L'utente chiede l'accesso ad un servizio del SP e seleziona l'IdP presso il quale ha l'identità digitale.
2. l SP invia una richiesta di autenticazione presso l'IdP di cui al punto 1.
3. L'IdP esegue la procedura di autenticazione e invia la risposta di autenticazione al SP.
4. Il SP richiede all'AA, informando l'utente in base alla normativa Privacy, gli attributi qualificati dei quali ha bisogno;
5. L'AA risponde direttamente al SP fornendo gli attributi richiesti.

4.2 Flusso applicativo che richiede il consenso dell'utente

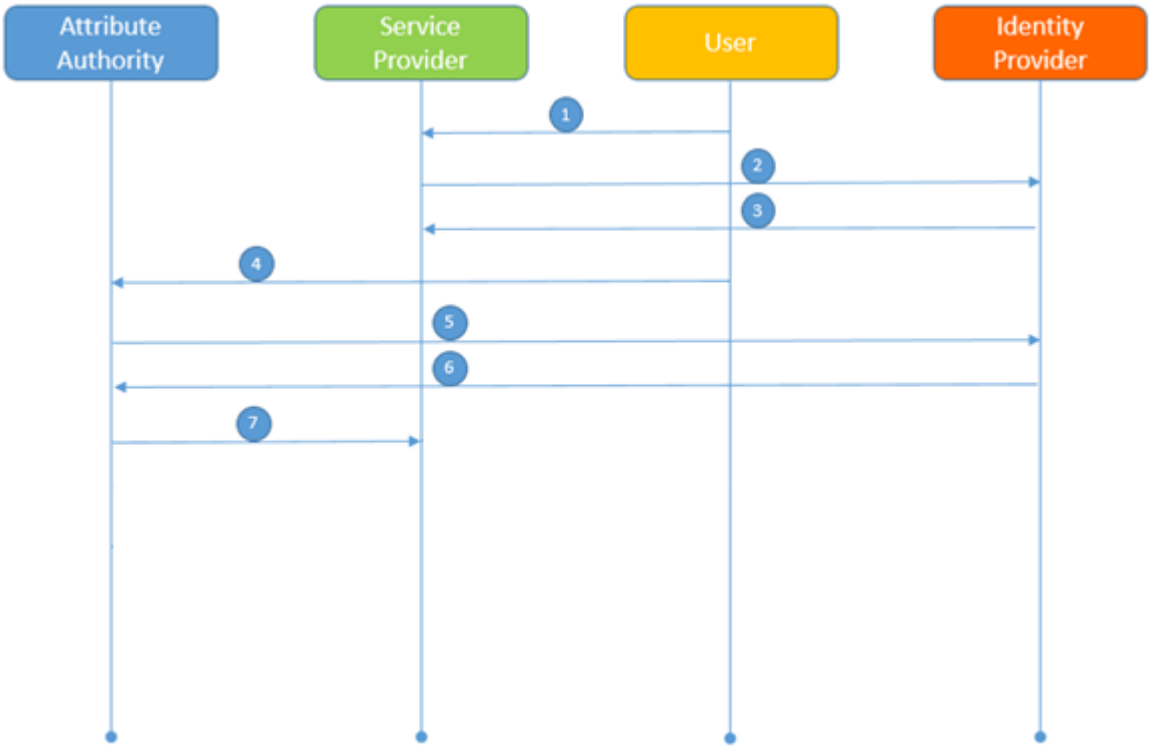

Figura 2 Flusso di richiesta di attributi qualificati con consenso.

Nel caso di richieste "sincrona" e "asincrona" (cfr. Figura 2):

1. L'utente chiede l'accesso ad un servizio del SP e seleziona l'IDP presso il quale ha l'identità digitale.
2. Il SP invia una richiesta di autenticazione presso l'IDP di cui al punto 1.
3. L'IDP esegue la procedura di autenticazione e invia la risposta di autenticazione al SP.
4. Il SP, avendo bisogno di uno o più attributi qualificati, si avvale dell'uso di una AA, informando l'utente secondo quanto previsto dalla sulla protezione dei dati personali.
5. L'AA identificata l'utente, ovvero richiede all'utente la prova di avvenuta autenticazione dell'utente presso l'IDP.
6. L'AA ottiene prova di avvenuta autenticazione e avvenuto consenso al rilascio dei dati presso il SP.
7. L'AA fornisce gli attributi qualificati dell'utente al SP.

Nel processo di autenticazione dell'utente, l'AA può richiedere all' IDP l'indirizzo di posta elettronica dell'utente, al fine di inviargli le seguenti comunicazioni via email:

- nel caso in cui l' AA abbia acquisito il consenso di lunga durata, dove è disponibile il servizio in rete accessibile tramite SPID per gestire (rinnovo o revoca) i consensi di lunga durata;
- all' approssimarsi della scadenza del consenso di lunga durata, informativa all' utente dell' imminente scadenza indicando il servizio in rete accessibile tramite SPID per poter eventualmente rinnovare il consenso secondo le modalità esposte al §5.3.2.

4.3 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 detto sistema di fiducia AA e SP possono verificare la firma dei messaggi scambiati con la controparte.

4.4 Servizio di consultazione per l'utente

Nel caso in cui sia previsto per norma e nel caso in cui siano consentite richieste di attributi continuative per mezzo di consenso di lunga durata, l'utente DEVE disporre di un servizio di consultazione tramite il quale, accedendovi tramite gli strumenti previsti dall'articolo 64 del CAD, può prendere visione delle trasmissioni dei propri dati personali (inclusi gli attributi qualificati) inviati a soggetti terzi ed esercitare i propri diritti legati al loro trattamento.

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

Con particolare riferimento ai consensi di lunga durata, se previsti dalla AA, accordati all'AA a seguito di richieste di attributi continuative, l'utente può usare servizi di consultazione per:

- verificare verso quali SP sono stati accordati tali consensi;

per ciascuno dei consensi di cui al punto precedente:

- verificare la data, l' ora e l' attestazione di attributi inviata per ciascuna delle richieste asincrone avvenuta entro il periodo concordato per effetto del consenso;
- accorciare la durata del consenso di lunga durata;
- revocare il consenso di lunga durata;

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

4.5 Registro delle Attribute Authority

L'articolo 16, comma 2, decreto del Presidente del Consiglio dei ministri 24 ottobre 2014 prevede che "L'Agenzia inserisce in un apposito registro, accessibile da parte dei fornitori di servizi, le tipologie di dati resi disponibili da ciascun gestore di attributi qualificati".

Presso il registro SPID è pubblicato un registro delle AA.

Per le AA basate su OAS3, nel registro SPID è reso disponibile il relativo documento OpenAPI.

Per la AA che gestisce le deleghe, amministrazioni di sostegno e tutele è reso disponibile un apposito metadata la cui struttura è pubblicata da AgID con apposito Avviso.

Vedi anche:

Allegato tecnico OAS3[3]

Allegato tecnico SAML[4]

[3] https://github.com/AgID/lg-spid-attribute-authority-docs/raw/master/LLGG_Attribute_Authority%E2%80%93Allegato_tecnico_OAS3.pdf
[4] https://github.com/AgID/lg-spid-attribute-authority-docs/raw/master/LLGG_Attribute_Authority%E2%80%93Allegato_tecnico_SAML.pdf