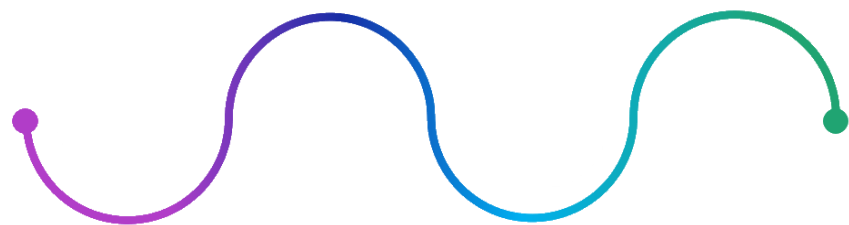


Università di Macerata – CDL Mediazione Linguistica

A.A. 2022/2023



14 ottobre 2022

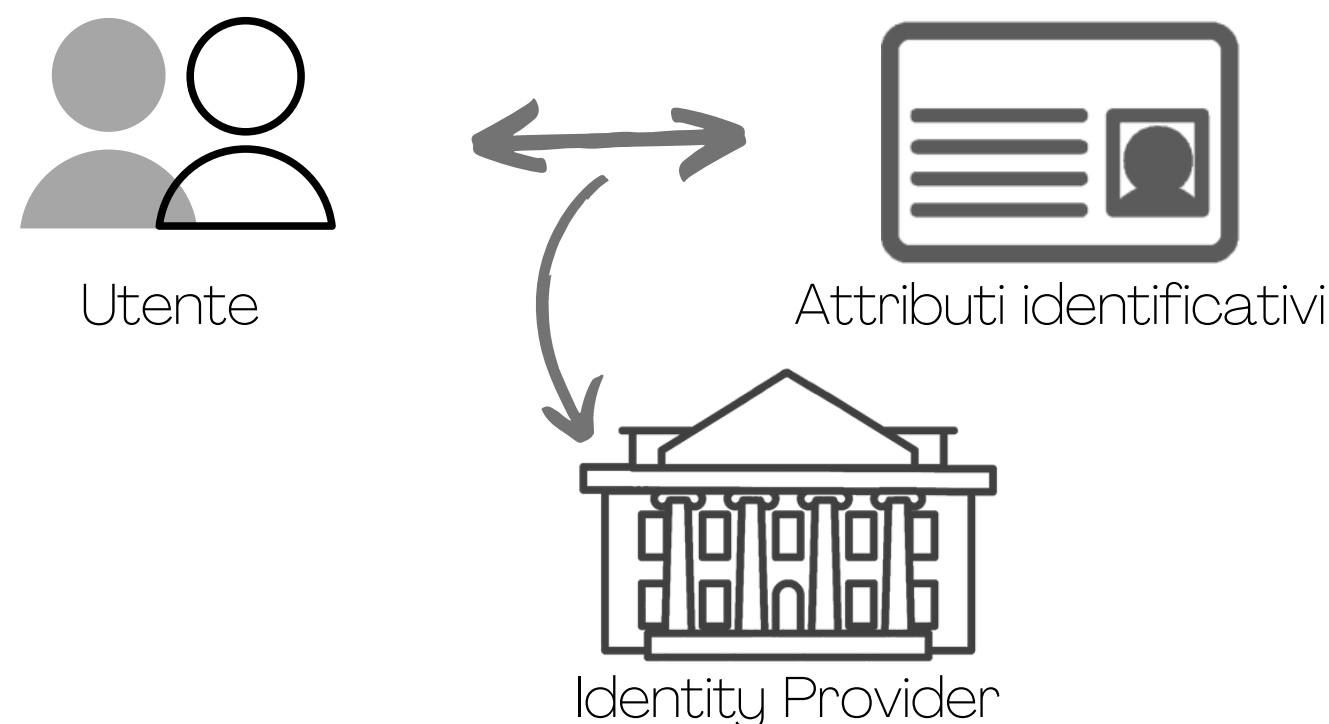


Identità digitale:

Definizione

Art. 1, CAD

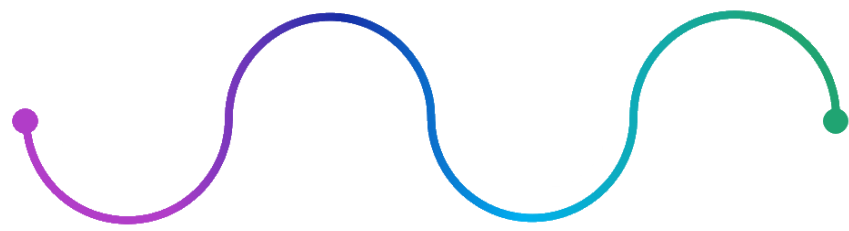
Identità digitale: rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale



Art. 3-bis, CAD

Cittadinanza digitale → Chiunque ha il diritto di accedere ai servizi online offerti dalle pubbliche amministrazioni, tramite la propria identità digitale e anche attraverso il Punto di accesso telematico (App IO) di cui all'art. 64-bis del CAD e nel Piano Triennale per la Pubblica Amministrazione

> Obiettivi: interagire con la PA e gestire l'identità digitale a livello europeo

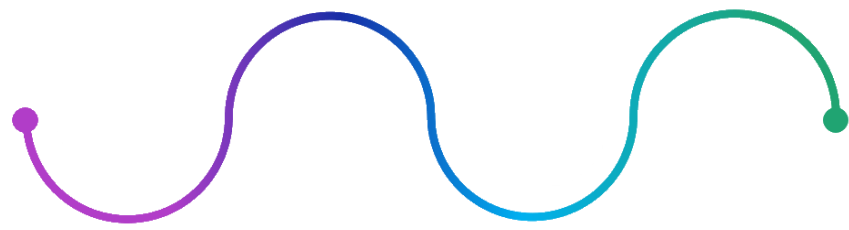


Sistema pubblico di gestione dell'identità digitale:

Definizione

A seguito dell'emanazione del [Regolamento eIDAS](#), l'Italia ha istituito lo **SPID**:
un [insieme aperto](#) di soggetti pubblici e privati (Identity Provider – IdP) che, previo accreditamento da parte dell'AgiD, identificano gli utenti per consentire loro l'accesso e la fruizione di servizi in rete.
> ogni soggetto può essere accreditato dall'AgiD previa dimostrazione del possesso dei requisiti da essa posti

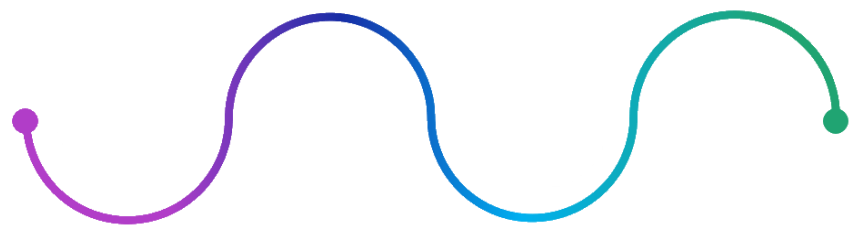
La **procedura di notifica** dello SPID agli altri Stati membri dell'UE, ai sensi del Regolamento eIDAS, è stata completata e, pertanto, a decorrere dal **10 settembre 2019** l'identità digitale SPID può essere usata per l'accesso ai servizi in rete di tutte le PPAA degli Stati membri.



Sistema pubblico di gestione dell'identità digitale: **Nodo eIDAS nazionale**

Tutte le PPAA che rendono accessibili i propri servizi online con credenziali SPID di livello 2 o 3 (come anche attraverso la carta di identità elettronica), hanno l'obbligo di rendere accessibili detti servizi anche con gli strumenti di autenticazione notificati dagli altri Stati membri, seguendo la procedura pubblicata sul sito dedicato al [nodo eIDAS nazionale](#) che connette tra loro tutte le PPAA nazionali per permettere ai cittadini UE l'accesso ai servizi.

> Gli enti che non si uniformano a queste modalità si espongono alla procedura di infrazione definita nel Reg. eIDAS.



SPID: I compiti dell'AgID

L'AgID ha il compito di:

- Accreditare i gestori dell'identità digitale (IdP) e i gestori di attributi qualificati (attestano il possesso di determinate caratteristiche dei soggetti dotati di SPID), stipulando con essi apposite convenzioni
- Curare l'aggiornamento del [Registro SPID](#) dei soggetti che operano nel sistema
- Vigilare sull'operato di tutti questi soggetti

In virtù dei compiti assegnati, con apposite Determinazioni, l'AgID ha:

- Definito le modalità attuative per la realizzazione dello SPID, i tempi e le modalità di adozione di SPID da parte delle PPAA e delle imprese, ed emanato le regole tecniche
- Stabilito le procedure necessarie per il rilascio dell'identità digitale da parte degli IdP, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID



SPID:

Accreditamento degli Identity Provider

Gli IdP gestiscono i servizi di registrazione e messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese, in qualità di soggetti giuridici.

I **requisiti** richiesti per l'accreditamento sono specificati nell'apposito Regolamento emanato dall'AglID.

Tra di essi si segnalano:

- l'affidabilità organizzativa, tecnica e finanziaria
- l'impiego di congruo personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie
- Il possesso delle certificazioni ISO 9001 (Qualità) e ISO 27001 (Sicurezza).

Inoltre, se il richiedente è un **soggetto privato** deve:

- avere forma giuridica di società di capitali e capitale sociale non inferiore a 5 milioni di euro
- garantire il possesso, da parte dei rappresentanti legali e delle figure dirigenziali, dei requisiti di onorabilità richiesti normalmente a chi amministra banche



SPID: Accreditamento degli Identity Provider

- > L'AgID ha emanato gli **schemi di convenzione** per l'adesione a SPID dei Gestori delle identità digitali e dei Fornitori privati di servizi che si impegnano a:
 - mantenere attivi i propri sistemi,
 - a perseguire una corretta gestione dell'identità
 - a perseguire il rispetto del Reg. eIDAS
 - a garantire l'interoperabilità a livello europeo
- > Nel mese di **novembre 2019** tutti gli IdP si sono impegnati a fornire per sempre ai cittadini, [gratuitamente](#), le credenziali SPID di livello 1 e 2
- > L'elenco degli Identity Provider accreditati è pubblicato nella [corrispondente sezione del sito AgID](#)



SPID: **Service Provider (SP)**

Erogano servizi ai soggetti identificati con SPID.

- I fornitori di servizi possono aderire allo SPID stipulando con l'AgID un'apposita convenzione, in cui vengono chiariti gli impegni reciproci e le condizioni di servizio e di interoperabilità a livello europeo
- I fornitori di servizi **conservano** per 24 mesi le informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi dai titolari di SPID

Le pubbliche amministrazioni aderiscono a SPID secondo le modalità stabilite dall'AgID e, in qualità di fornitori dei servizi, usufruiscono **gratuitamente** delle verifiche rese disponibili dagli IdP e dai gestori di attributi qualificati. Pertanto, le PPAA non sostengono costi per consentire l'autenticazione con SPID



SPID: **Soggetti aggregatori**

PPAA o soggetti privati che offrono a terzi (soggetti aggregati) la possibilità di rendere accessibili tramite lo SPID i rispettivi servizi.

Essi si distinguono in:

- aggregatori di servizi pubblici (es: sistema di autenticazione regionale)
- aggregatori di servizi privati

I soggetti aggregatori possono svolgere per il soggetto aggregato solo la funzione di autenticazione con SPID oppure ospitare l'intero servizio.



SPID: **Registration Authority Officer (RAO)**

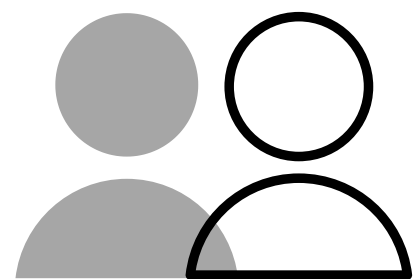
I cittadini possono recarsi anche presso le PPAA per ottenere lo SPID.

> Su richiesta di alcune PPAA locali, l'AglD ha emanato le Linee Guida per il modello di RAO pubblico, consentendo alle pubbliche amministrazioni interessate di svolgere questa importante attività sul territorio, tipicamente presso gli sportelli pubblici.

Il cittadino può recarsi a uno sportello pubblico e avviare la procedura per il rilascio di SPID



SPID: Soggetti del sistema SPID



utente: può disporre di una o più identità digitali contenenti alcune informazioni identificative obbligatorie, come il codice fiscale, il nome, il cognome, il luogo e data di nascita



spid



gestore dell'identità digitale: deve essere accreditato dall'AglD e crea e rilascia le identità digitali, previa identificazione dell'utente



gestore di attributi qualificati: può certificare attributi qualificati, come il possesso di un titolo di studio o l'appartenenza a un ordine professionale



fornitore di Servizi
(pubblico o privato) eroga servizi online, previo riconoscimento dell'utente da parte del gestore dell'identità digitale



SPID: **Registro SPID**

Contiene le informazioni relative ai soggetti che hanno in corso un'apposita convenzione con AgID per operare nell'ambito dello SPID e assolve la funzione di registro di federazione, certificando la relazione di fiducia stabilita tra i **soggetti appartenenti a SPID**. Tale relazione di fiducia si fonda sulla condivisione dei criteri di sicurezza e delle regole di interoperabilità previste da SPID

- > viene gestito da AgID
- > è accessibile a livello nazionale e internazionale



SPID: Rilascio dell'identità digitale

L'utente interessato:

invia all'IdP un modulo di **richiesta di adesione** contenente:

- a) i suoi dati identificativi, che costituiscono gli **attributi identificativi** dell'identità digitale
- b) le informazioni che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali e il richiedente dell'identità digitale, che costituiscono gli **attributi secondari** dell'identità digitale

Al ricevimento della richiesta, il gestore dell'identità digitale procede all'**identificazione del soggetto** richiedente, che consiste nell'accertamento delle informazioni sufficienti a identificarlo.

Questa operazione di identificazione della persona fisica può essere effettuata:

- a)** a vista in presenza tramite la carta d'identità;
- b)** a vista in digitale da remoto tramite strumenti di registrazione audio/video;
- c)** con strumenti di identificazione informatica (CIE, CNS, TS-CNS, altra identità SPID);
- d)** mediante firma elettronica qualificata o firma digitale



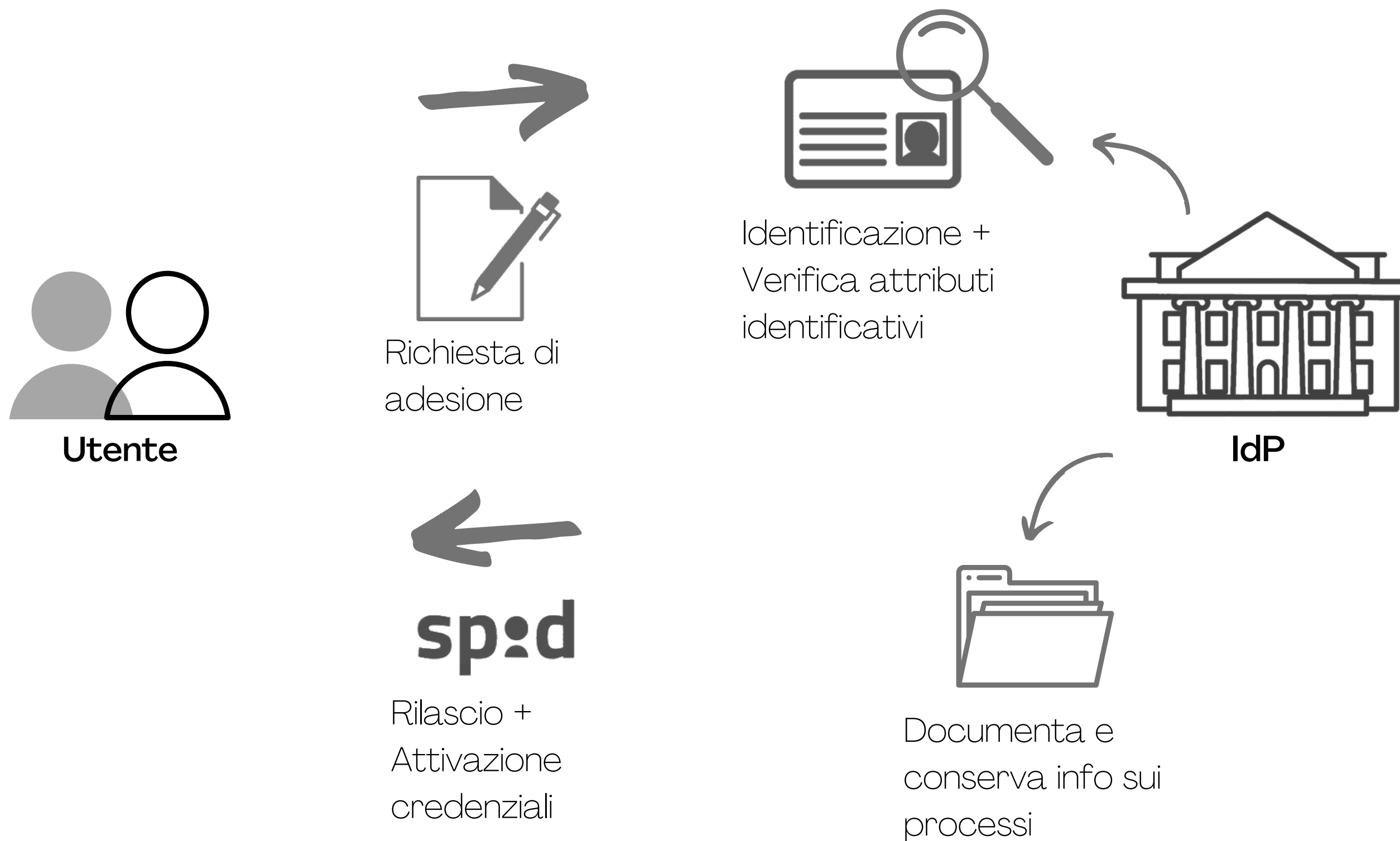
SPID:

Rilascio dell'identità digitale

1. All'identificazione del soggetto richiedente segue la **verifica dell'identità dichiarata**, che consiste nel rafforzamento del livello di attendibilità degli attributi di identità, raccolti in fase di identificazione, compiuta attraverso **accertamenti** effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti. (Es: ANPR)
2. Sia il processo di identificazione che il processo di verifica sono eseguiti allo scopo di ottenere un adeguato grado di **affidabilità**, tenuto conto anche dello specifico livello di sicurezza di SPID
3. I gestori dell'identità digitale, al fine di poter **documentare** la corretta esecuzione dei processi relativi all'attività di rilascio, conservano i riscontri relativi alle operazioni di identificazione e verifica.
4. In sede di vigilanza l'AglID valuta l'**adeguatezza dei processi** di registrazione e conservazione e ne verificano l'effettiva applicazione
5. Espletate con successo tutte le attività previste dai processi precedenti, l'identità digitale viene **creata e rilasciata** dal gestore. La consegna delle credenziali deve essere operata con modalità e strumenti che assicurino che la stessa sia effettuata al legittimo destinatario e siano salvaguardati la riservatezza e il contenuto
6. L'**attivazione delle credenziali** è il processo durante il quale le credenziali, o i mezzi usati per produrle, sono rese effettivamente operative e pronte all'utilizzo



SPID: Rilascio dell'identità digitale





SPID: **Ciclo di vita dell'identità digitale**

L'utente è tenuto a mantenere **aggiornati**, in maniera proattiva o a seguito di segnalazione da parte del gestore, i contenuti degli attributi identificativi. Le modalità operative per gli aggiornamenti devono essere rese possibili attraverso un'[area web accessibile](#) mediante le credenziali SPID. Ad ogni variazione degli attributi relativi a un'identità, il gestore, prima di aggiornare i dati, esegue le fasi di [esame](#) e [verifica](#) in relazione al livello SPID associato all'identità digitale.

Il gestore **revoca l'identità digitale** nei casi seguenti:

- a. risulta non attiva per un periodo superiore a 24 mesi;
- b. per decesso della persona fisica;
- c. per estinzione della persona giuridica;
- d. per uso illecito dell'identità digitale;
- e. per richiesta dell'utente;
- f. per scadenza contrattuale;
- g. per scadenza documento identità collegato a SPID

I gestori dell'identità digitale **conservano la documentazione** inerente al processo di adesione per un periodo pari a 20 anni decorrenti dalla revoca dell'identità digitale



SPID: **Autenticazione tramite SPID**

Il processo di autenticazione informatica è diretto alla verifica dell'identità digitale associata a un soggetto ai fini dell'erogazione di un servizio online.

> A tale processo è associato un **livello di sicurezza o di garanzia** (detto *level of assurance* - LoA - Standard ISO 29115) che fa riferimento all'intero processo, dalla preliminare associazione tra soggetto e identità digitale, al rilascio e dall'identificazione all'erogazione del servizio.



SPID:

Livelli di sicurezza delle identità digitali

SPID è basato su **tre livelli** di sicurezza di autenticazione informatica.

1. Nel **primo livello** (Level of Assurance 2) , il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a un **singolo fattore** (password). Questo livello è applicabile nei casi in cui il danno causato da un utilizzo improprio dell'identità digitale abbia un **basso impatto** per le attività del cittadino, dell'impresa e della PA
2. Il **secondo livello** (Level of Assurance 3) è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche tali da ridurre significativamente il rischio di uso abusivo o di alterazione di identità. A tale livello è associato un **rischio notevole** e compatibile con l'impiego di un sistema di autenticazione informatica a **due fattori** non necessariamente basato su certificati digitali (sistema OTP hardware o software). Questo livello è adeguato ai casi in cui un indebito utilizzo dell'identità digitale può provocare un danno consistente
3. Il **terzo livello** (Level of Assurance 4) è compatibile con l'impiego di un sistema di autenticazione informatica a **due fattori** basato su **certificati digitali** e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato II del Reg. eIDAS. Questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un **danno grave**.



Sistema SPID:

Livelli di sicurezza delle identità digitali

La scelta del livello di identità SPID minimo necessario per accedere ai servizi erogati da un SP [competente allo stesso Service Provider](#), e non deve discriminare l'accesso sulla base del gestore di identità che l'ha fornita.

- > La metodologia suggerita dall'AgID prevede l'**identificazione dei rischi** per ogni specifico servizio e la conseguente **assegnazione dei livelli di sicurezza** previsti in ambito SPID; ovviamente la misura dell'impatto potenziale dei rischi individuati dipende dallo specifico contesto e dalle entità coinvolte da un'impropria autenticazione
- > è importante svolgere una **PROGETTAZIONE** preliminare



Sistema SPID:

Fasi del processo di autenticazione con SPID

Per il processo di autenticazione informatica, SPID adotta il modello federato delle identità digitali definito dalle specifiche SAML (Security Assertion Markup Language) emesse dal consorzio OASIS.

Passaggi previsti:

Fase 1 - il titolare dell'identità digitale:

- richiede l'accesso a un servizio collegandosi al portale del fornitore di servizi
- sceglie il suo IdP dall'apposito Registro SPID che viene visualizzato

Fase 2 - il fornitore di servizi:

- indirizza il soggetto titolare dell'identità digitale verso l'IdP individuato
- richiede l'autenticazione con il livello SPID associato al servizio richiesto e l'eventuale attestazione di attributi necessari per l'autorizzazione all'accesso

Fase 3 - il gestore dell'identità digitale:

- verifica l'identità del soggetto sulla base di credenziali fornite dallo stesso
- in caso di esito positivo emette un'asserzione di autenticazione SAML* attestante gli attributi richiesti

Fase 4 - il titolare dell'identità digitale viene quindi reindirizzato, portando con sé l'asserzione prodotta, verso il SP.

*Documento XML contenente dati che confermano al fornitore di servizi che la persona che sta effettuando l'accesso è stata autenticata.



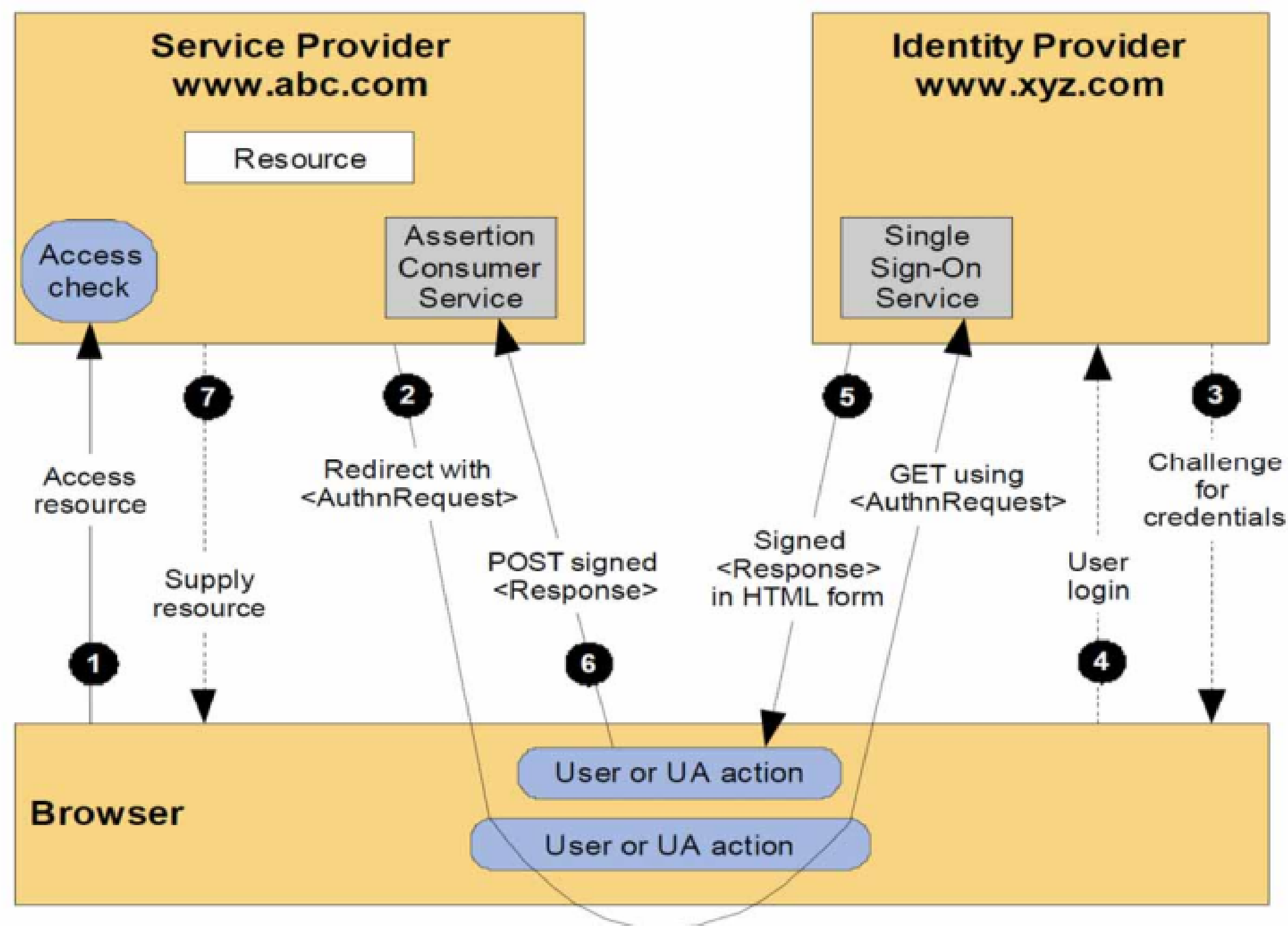
Sistema SPID:

Fasi del processo di autenticazione con SPID

Fase 5: se il SP deve verificare **attributi qualificati** riferibili all'utente:

- individua, tramite il registro SPID, il relativo gestore e gli inoltra una richiesta di attestazione;
- in risposta alla sua richiesta, riceve un'asserzione SAML con gli attributi qualificati

Fase 6: il SP **raccoglie tutte le necessarie asserzioni SAML** e decide se accettare o rigettare la richiesta di accesso





Sistema SPID: **Utilizzo dell'identità digitale SPID**

Per la sicurezza del canale di comunicazione tra utente e gestore è necessario che il gestore IdP garantisca la **cifratura** con algoritmi aggiornati alle versioni più recenti e renda possibile l'utilizzo delle funzionalità di accesso web mediante le tipologie di browser più diffuse ma con limitazioni per le versioni più obsolete

> Per le identità digitali di livello 2 e 3, allo scopo di garantire la massima sicurezza e stabilità del sistema, non si prevede la possibilità di mantenere sessioni di autenticazione condivise



Sistema SPID:

Registro delle transazioni del fornitore di servizio

I SP sono obbligati a **conservare per 24 mesi** le informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi. Tali informazioni consistono nella registrazione di:

- [messaggio SAML](#) di richiesta di autenticazione;
- relativa asserzione emessa dal gestore delle identità.

Tali messaggi sono firmati, rispettivamente, dal SP e dall'IdP.

- L'insieme delle Registrazioni costituisce il **Registro delle transazioni** del fornitore del servizio.
- Le registrazioni devono avere caratteristiche di riservatezza, inalterabilità e integrità.

Analogo registro dovrà essere tenuto dal gestore delle identità digitali