Identità digitale

SAML & OAuth

Introduzione

L'identità digitale è l'insieme delle risorse digitali associate in maniera univoca ad una persona fisica che la identifica, rappresentandone la volontà, durante le sue attività digitali.

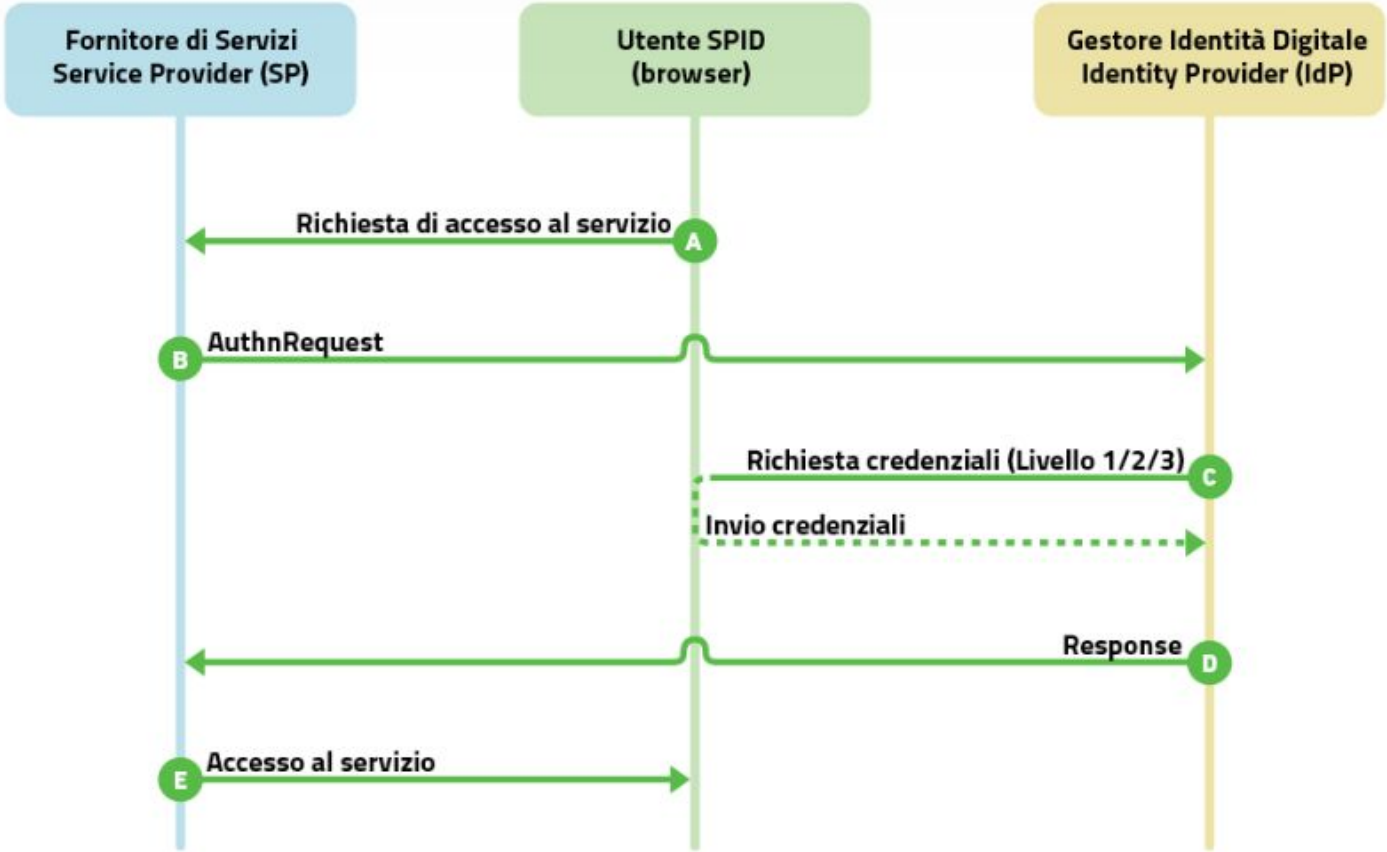
Possibili modelli per garantire l’identità digitale

- Firma digitale
- Certificato digitale
- SAML
- OAuth

SAML

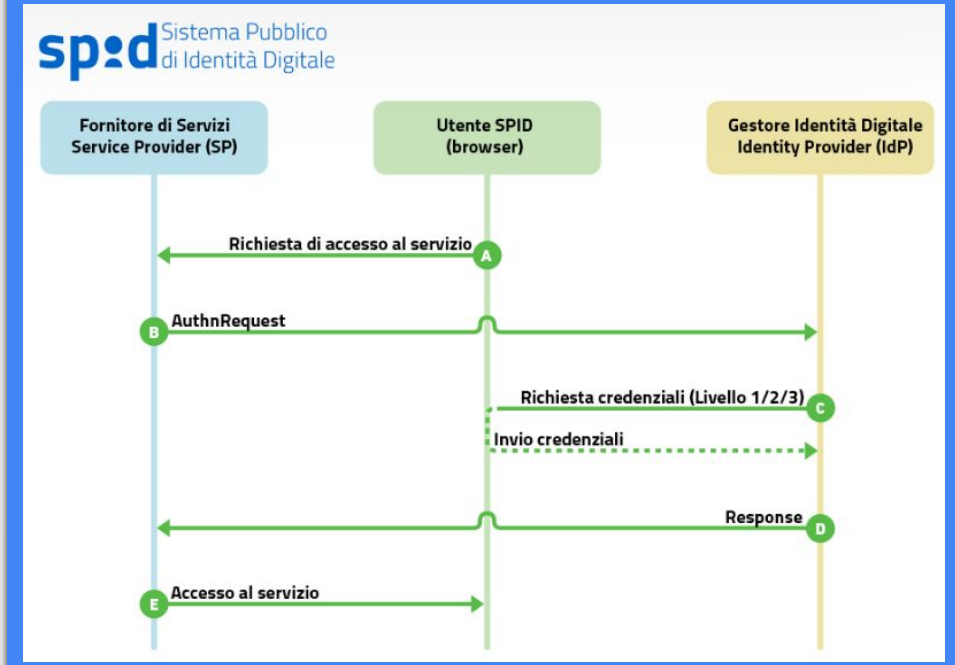
SAML (Security Assertion Markup Language) è uno standard per lo scambio di dati di **autenticazione**, il problema principale che SAML cerca di risolvere è quello dell' SSO (Web Single sign-on), traducibile come "autenticazione unica" o "identificazione unica" ovvero la proprietà di un sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

spid Sistema Pubblico di Identità Digitale



- Gestore delle identità (Identity Provider o **IdP**) che gestisce gli utenti e la procedura di autenticazione;

- Fornitore di servizi (Service Provider o **SP**) che, dopo aver richiesto l'autenticazione dell'utente all'Identity Provider, ne gestisce l'autorizzazione sulla base degli attributi restituiti dal Gestore dell'identità, ed eroga il servizio richiesto

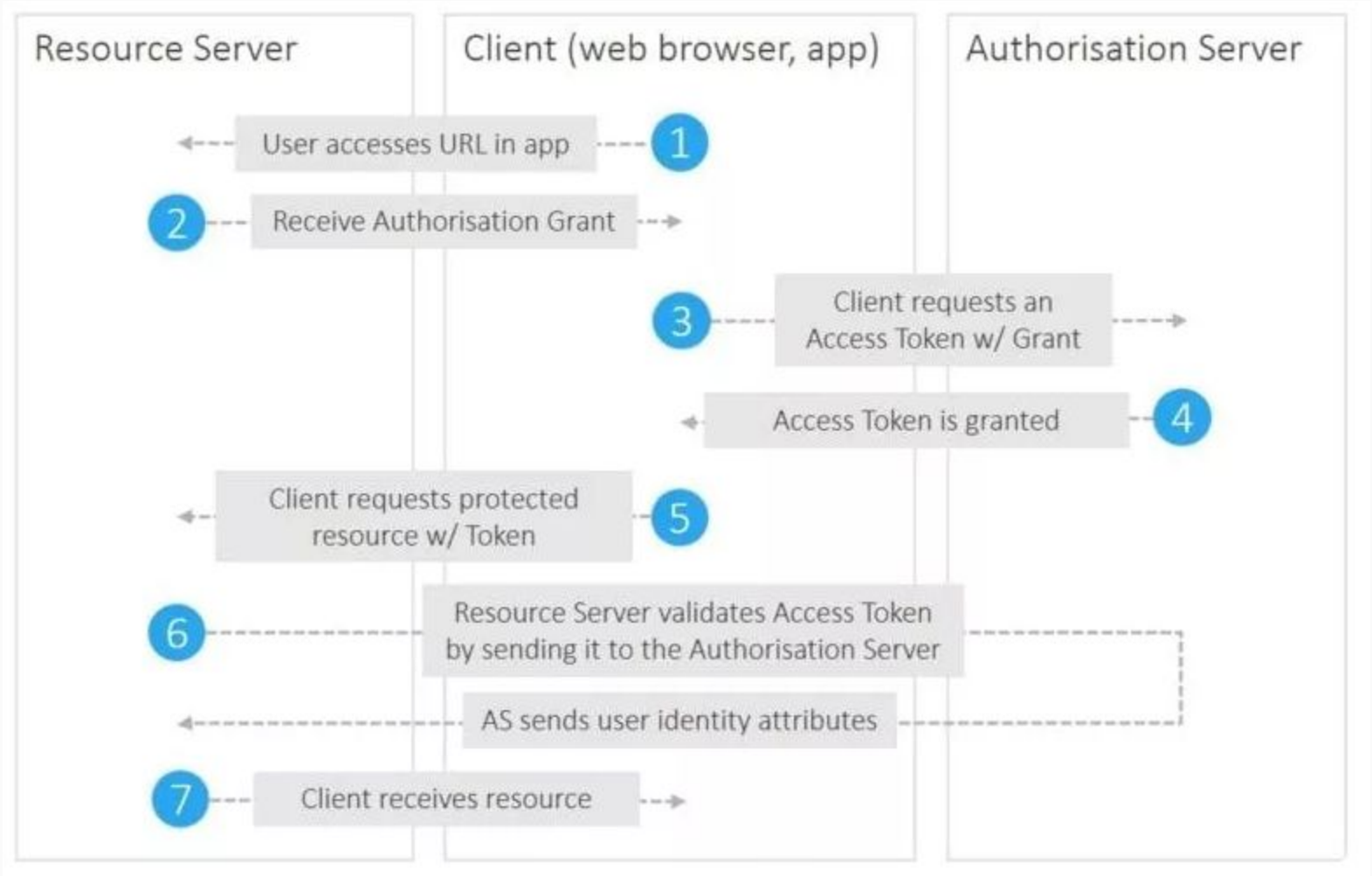


Esempio IdP Poste Italiane

https://www.poste.it/posteid.html

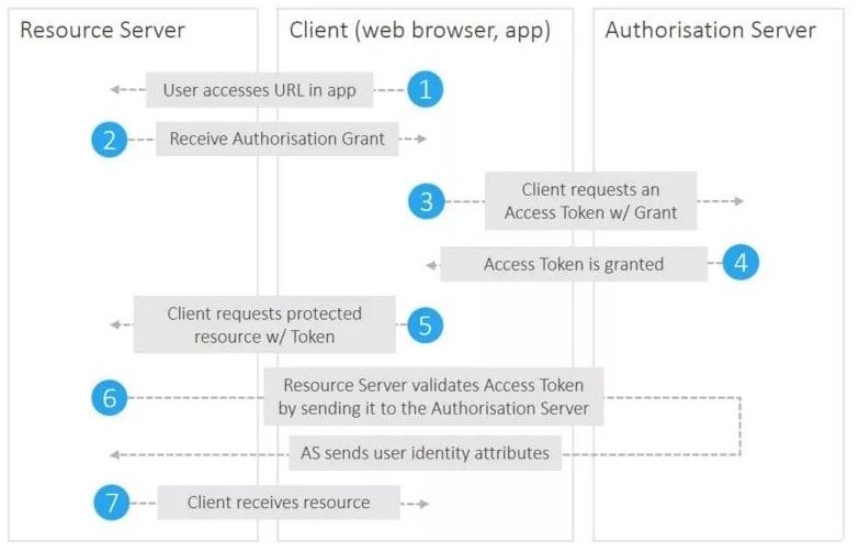
OAuth2

OAuth (Open **Authorization**), è uno standard progettato per consentire a un sito web o un'applicazione di accedere a risorse ospitate da altre applicazioni web per conto di un utente, fornisce quindi un accesso consentito e limita le azioni di ciò che l'applicazione client può eseguire sulle risorse per conto dell'utente, senza mai condividere le credenziali dell'utente.


Resource Server
Client (web browser, app)
Authorisation Server
User accesses URL in app
1
2
Receive Authorisation Grant
3
Client requests an Access Token w/ Grant
Access Token is granted
4
Client requests protected resource w/ Token
5
6
Resource Server validates Access Token by sending it to the Authorisation Server
AS sends user identity attributes
7
Client receives resource

- **Proprietario della risorsa**: L'utente o il sistema che possiede le risorse protette e può concedere l'accesso ad esse.

- **Client**: Il client è il sistema che richiede l'accesso alle risorse protette. Per accedere alle risorse, il client deve possedere il Token di accesso appropriato.



- **Server di autorizzazione** (Authorization Server): riceve le richieste dal client per i token di accesso e li emette dopo aver ottenuto l'autenticazione e il consenso da parte del proprietario della risorsa.

- **Server delle risorse** (Resource Server): protegge le risorse dell'utente e riceve le richieste di accesso dal client. Accetta e convalida un Token di accesso dal Client e gli restituisce le risorse appropriate.