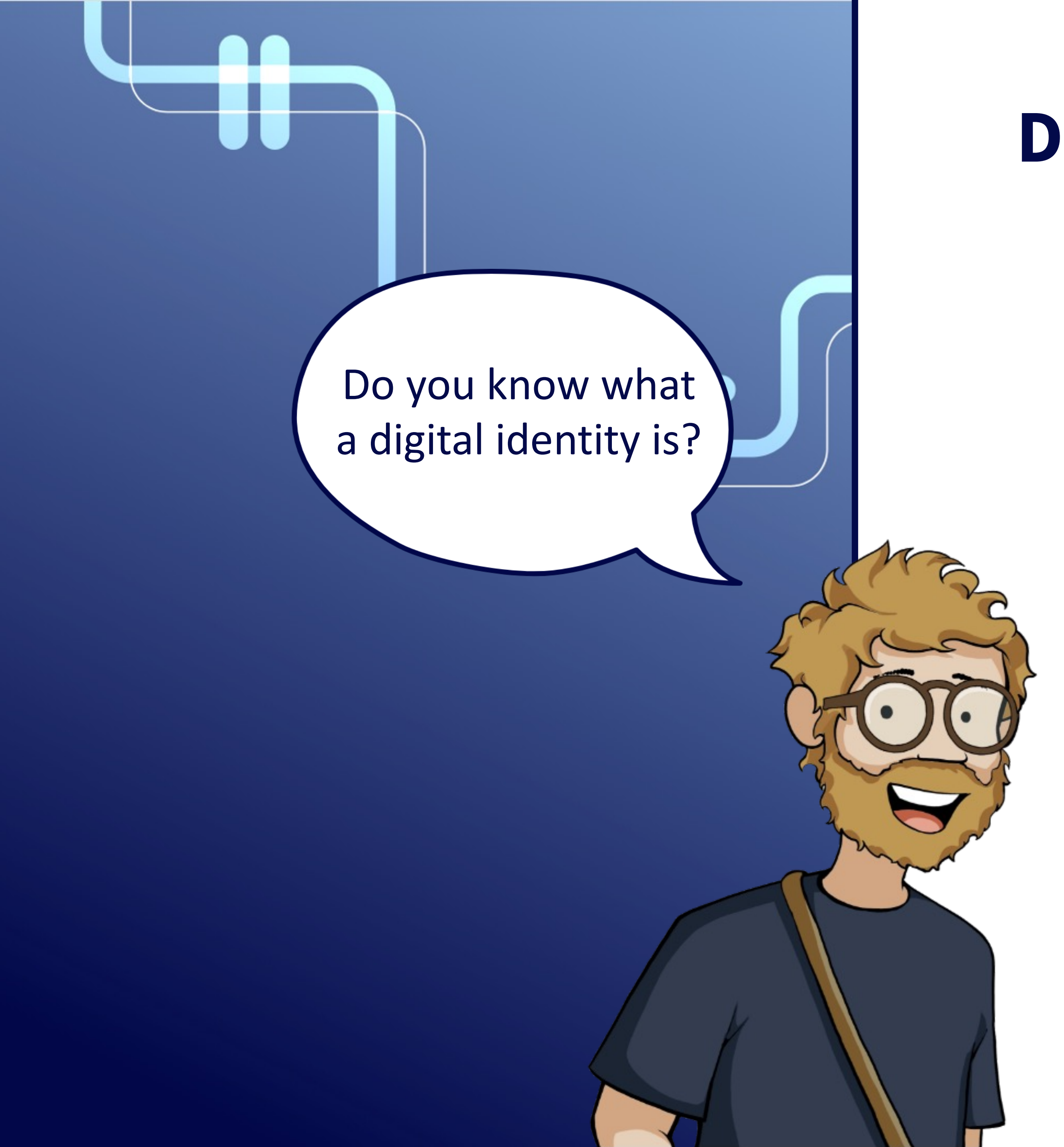
VERY TECH TRIP TALK

Powered by OVHcloud

One identity to federate them all!

Seb Ferrer
Nicolas Fournier

2 février 2022



Digital identities

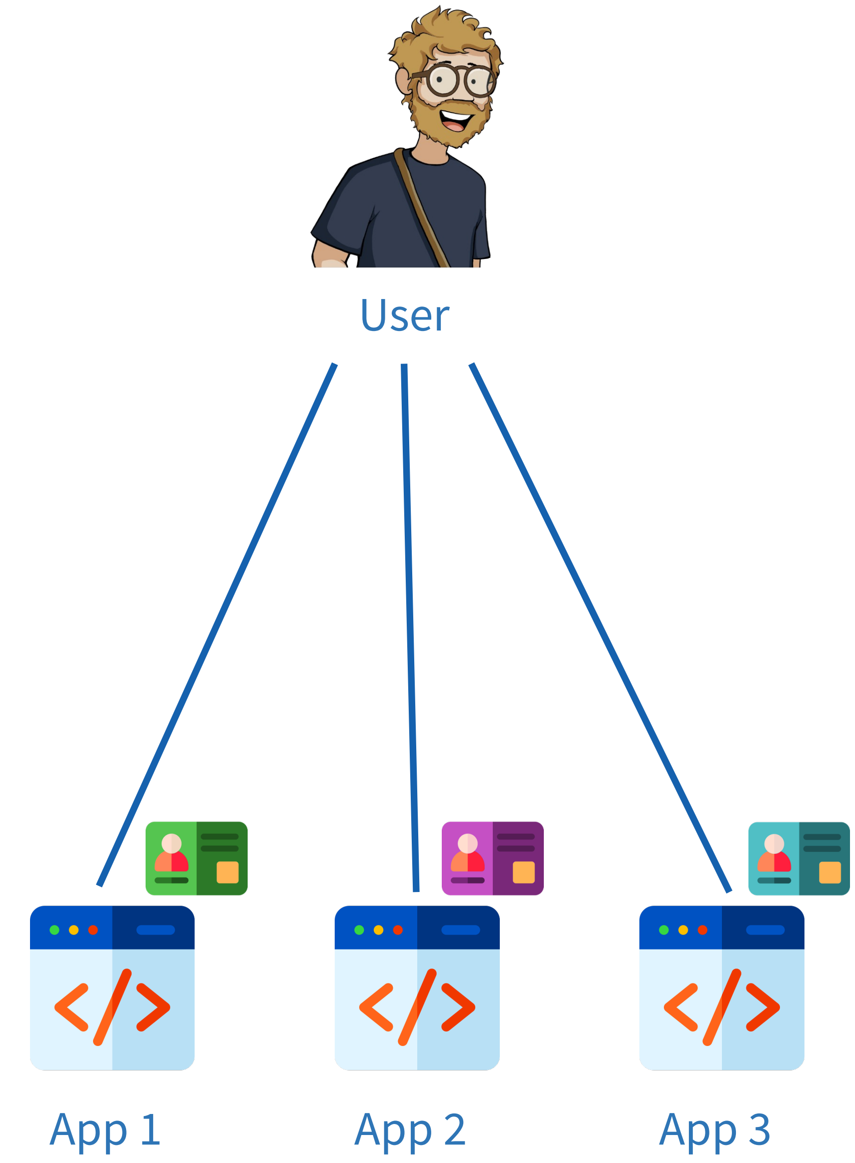
Link between:

- Real entity (person, organization, company)
- Virtual entity (digital representation)

Let's talk about authentication

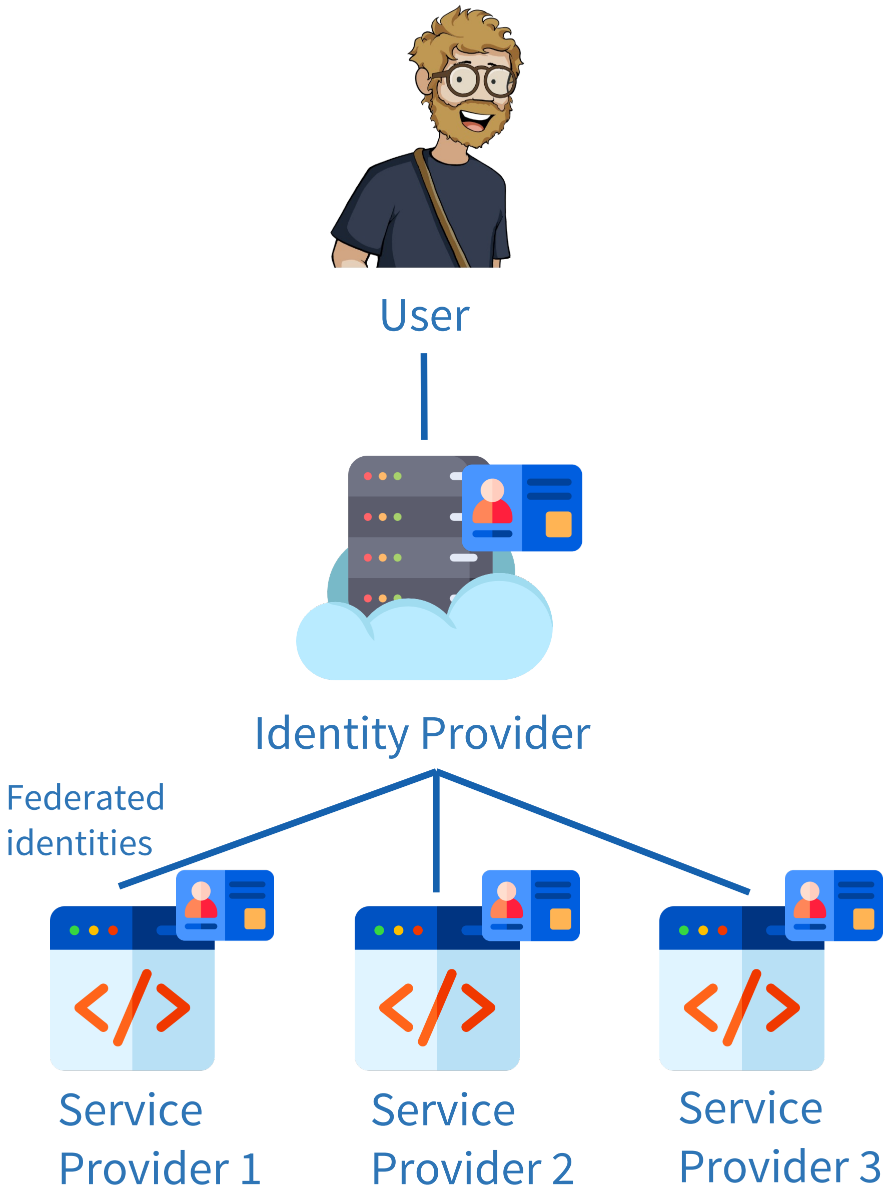
Authentication

- User experience
- Administrator experience
- Attack surface
- Security features



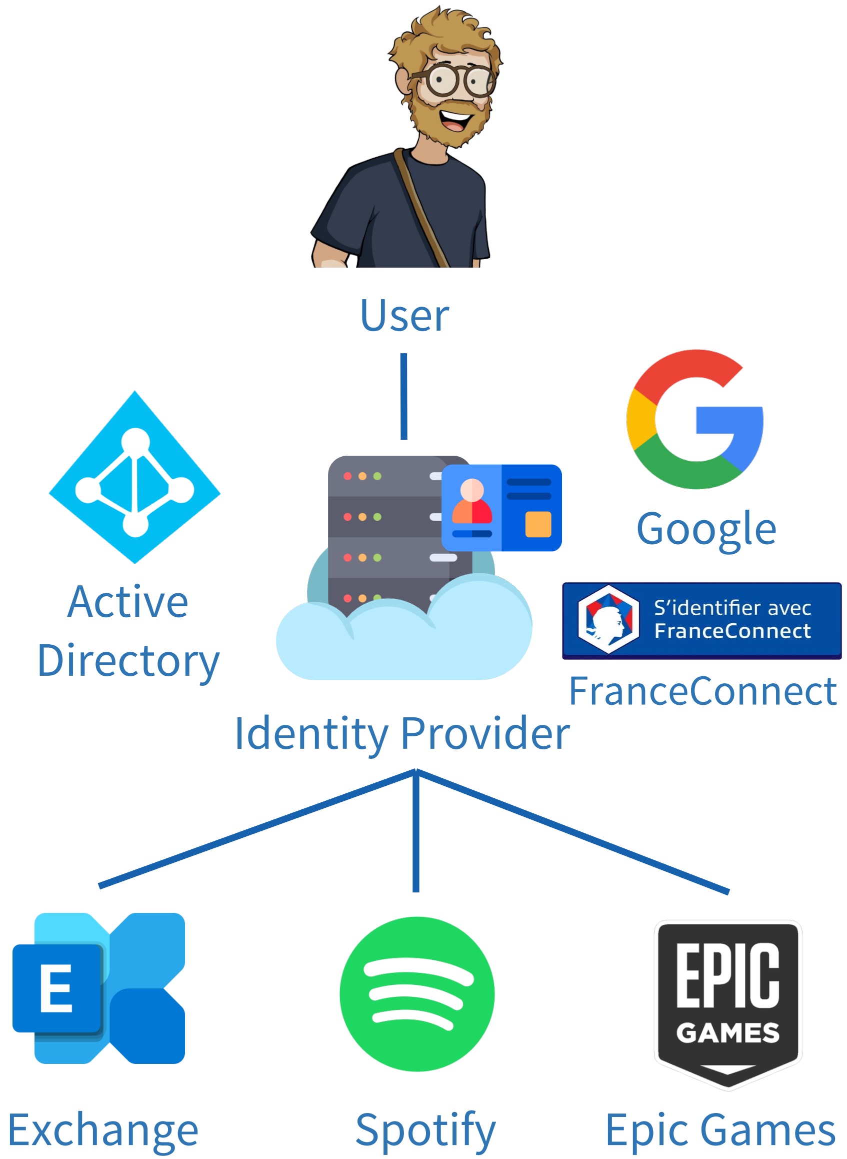
Authentication

- User experience
- Administrator experience
- Attack surface
- Security features

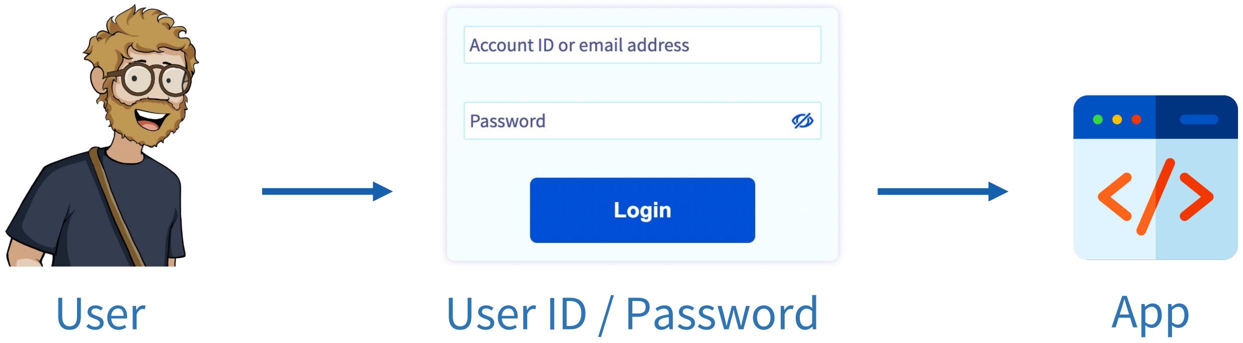


Authentication

- User experience
- Administrator experience
- Attack surface
- Security features

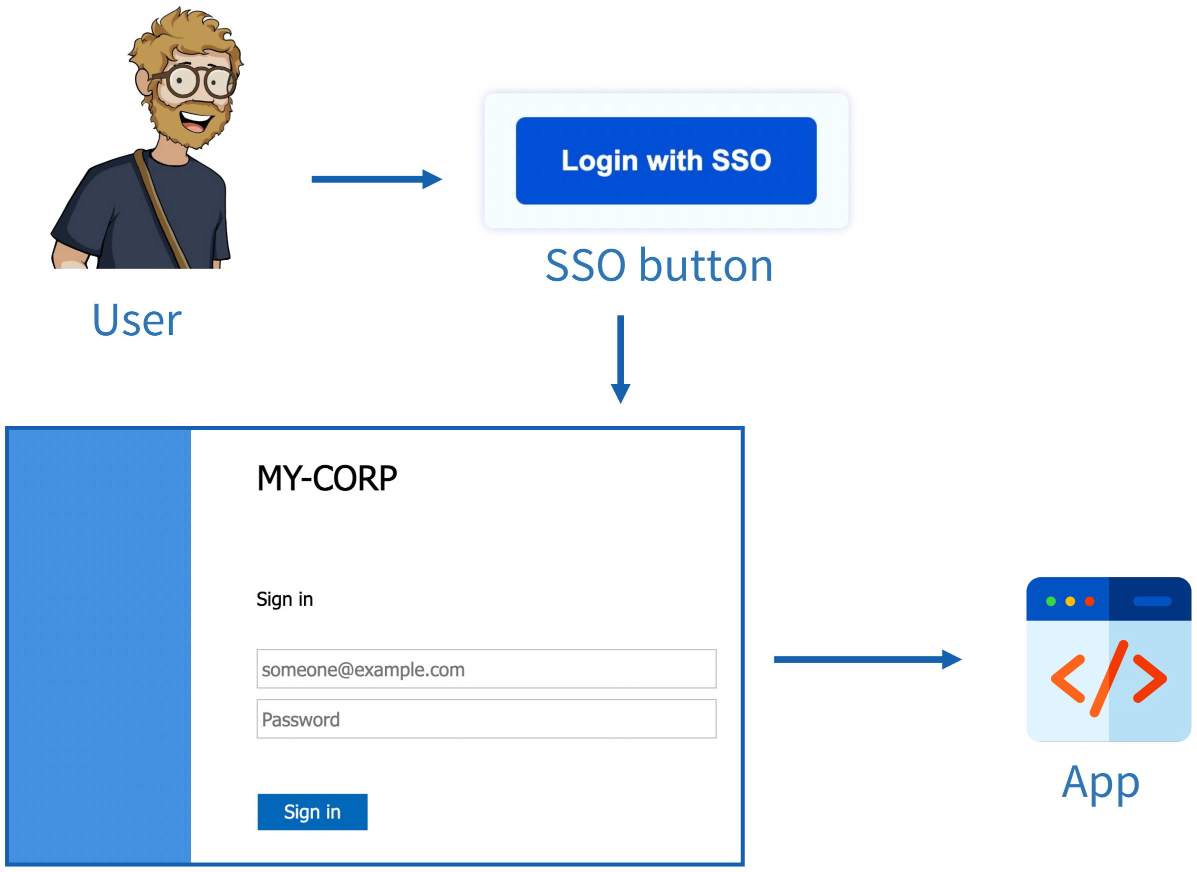


Classic login flow



- One identity per application for each user
- App responsible for authentication
- Different login/password per app

Login flow through federation



User

SSO button

MY-CORP

Sign in

someone@example.com

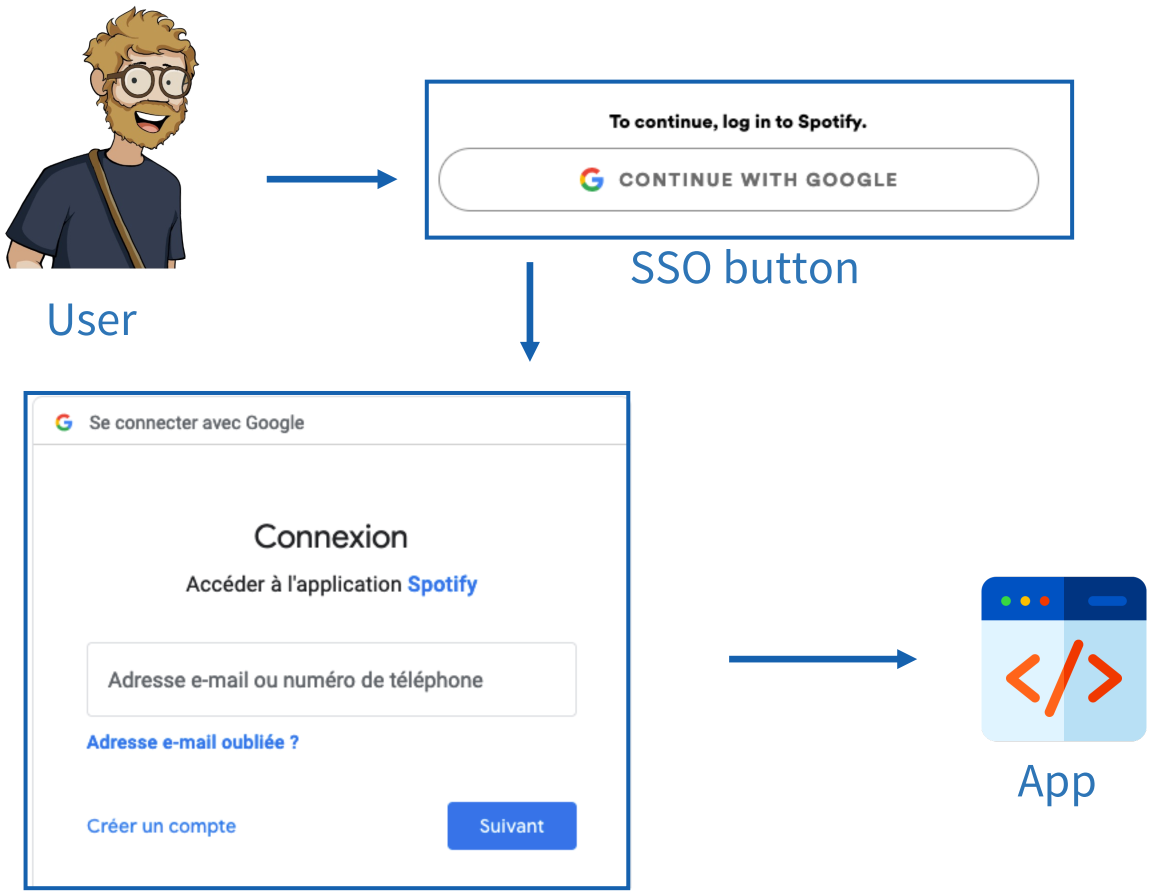
Password

App

Identity Provider login (Active Directory)

- One centralized identity for each user
- Delegated authentication
- Single login/password

Login flow through federation



User

To continue, log in to Spotify.

CONTINUE WITH GOOGLE

SSO button

Se connecter avec Google

Connexion

Accéder à l'application Spotify

Adresse e-mail ou numéro de téléphone

Adresse e-mail oubliée ?

Créer un compte

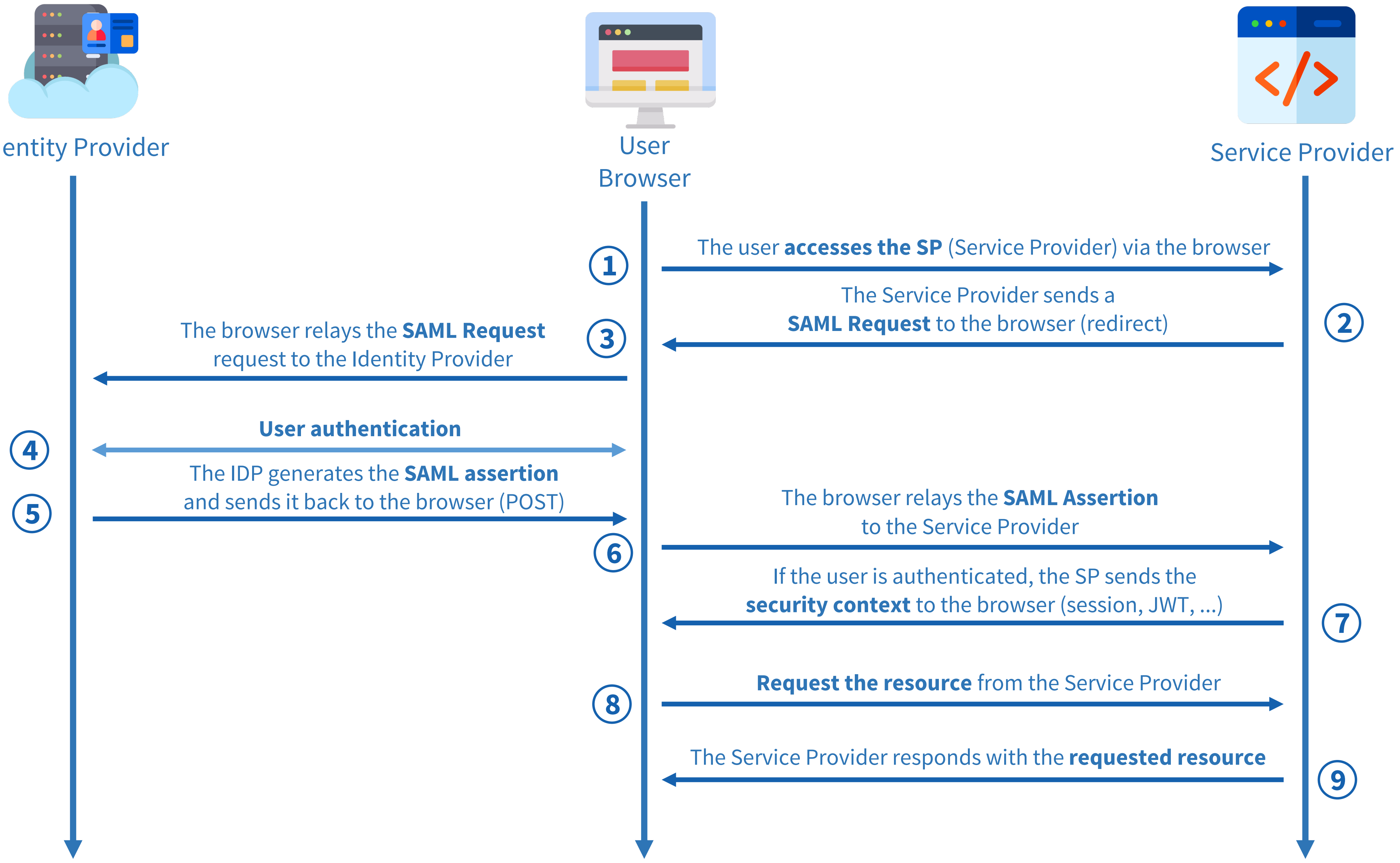
Suivant

Identity Provider login (Google)

App

- One centralized identity for each user
- Delegated authentication
- Single login/password

SAML flow



Identity Provider

User Browser

Service Provider

1 The user **accesses the SP** (Service Provider) via the browser

2 The Service Provider sends a **SAML Request** to the browser (redirect)

3 The browser relays the **SAML Request** request to the Identity Provider

4 **User authentication**

5 The IDP generates the **SAML assertion** and sends it back to the browser (POST)

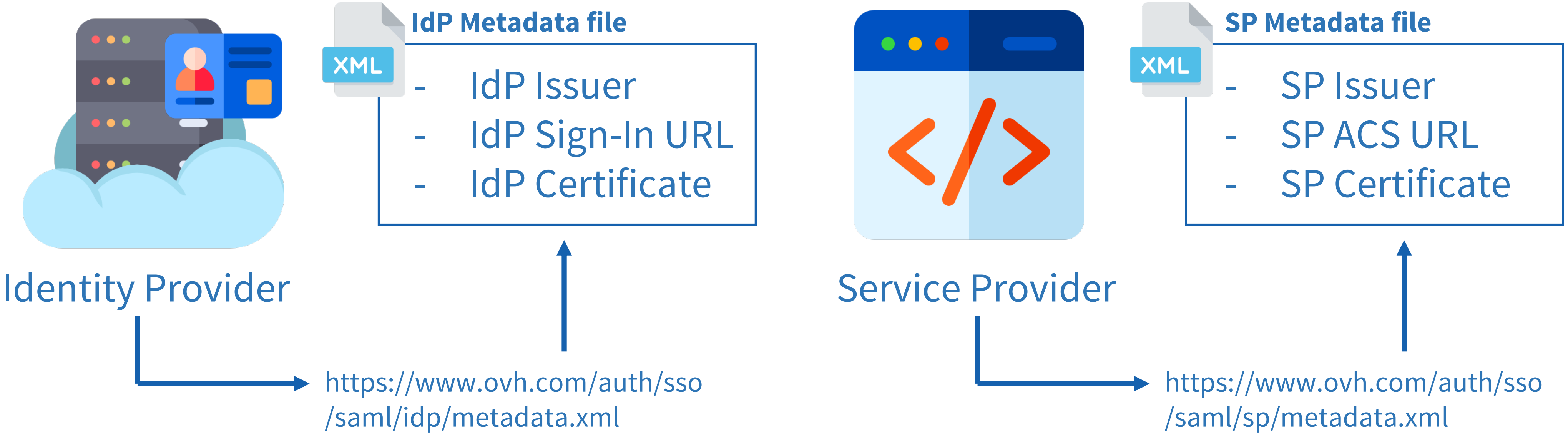
6 The browser relays the **SAML Assertion** to the Service Provider

7 If the user is authenticated, the SP sends the **security context** to the browser (session, JWT, ...)

8 **Request the resource** from the Service Provider

9 The Service Provider responds with the **requested resource**

SAML Trust



Provides to SP:

IdP Metadata file

- IdP Issuer
- IdP Sign-In URL
- IdP Certificate

Identity Provider

https://www.ovh.com/auth/sso
/saml/idp/metadata.xml

Provides to IdP:

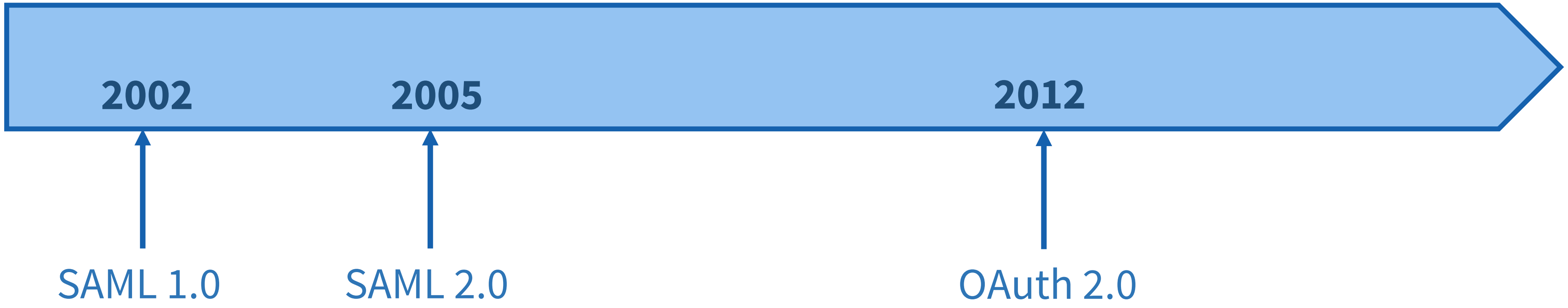
SP Metadata file

- SP Issuer
- SP ACS URL
- SP Certificate

Service Provider

https://www.ovh.com/auth/sso
/saml/sp/metadata.xml

Brief history



2002

SAML 1.0

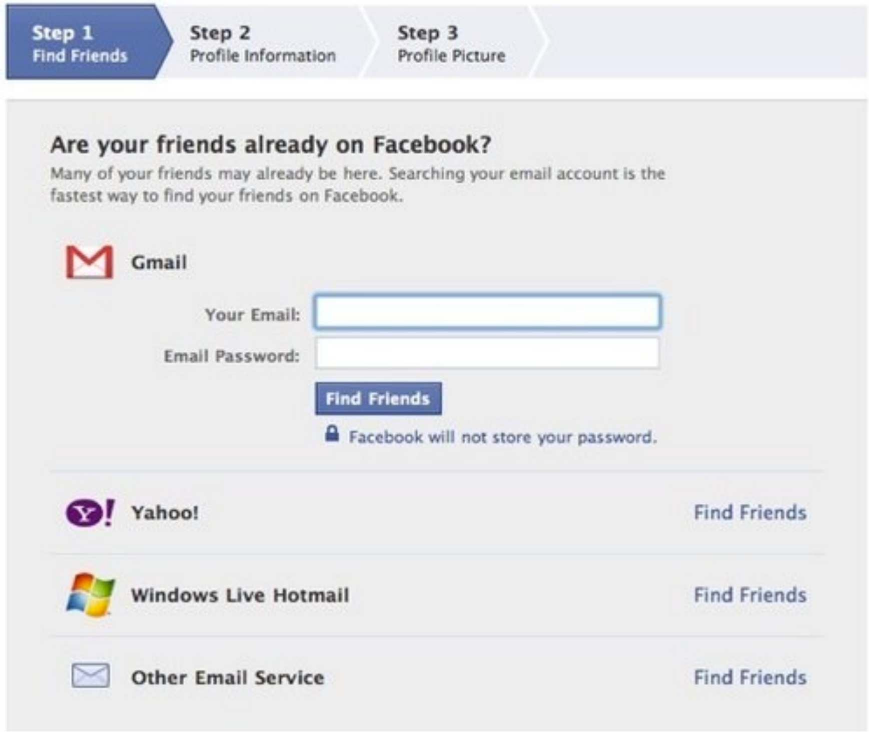
2005

SAML 2.0

2012

OAuth 2.0

OAuth 2



Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

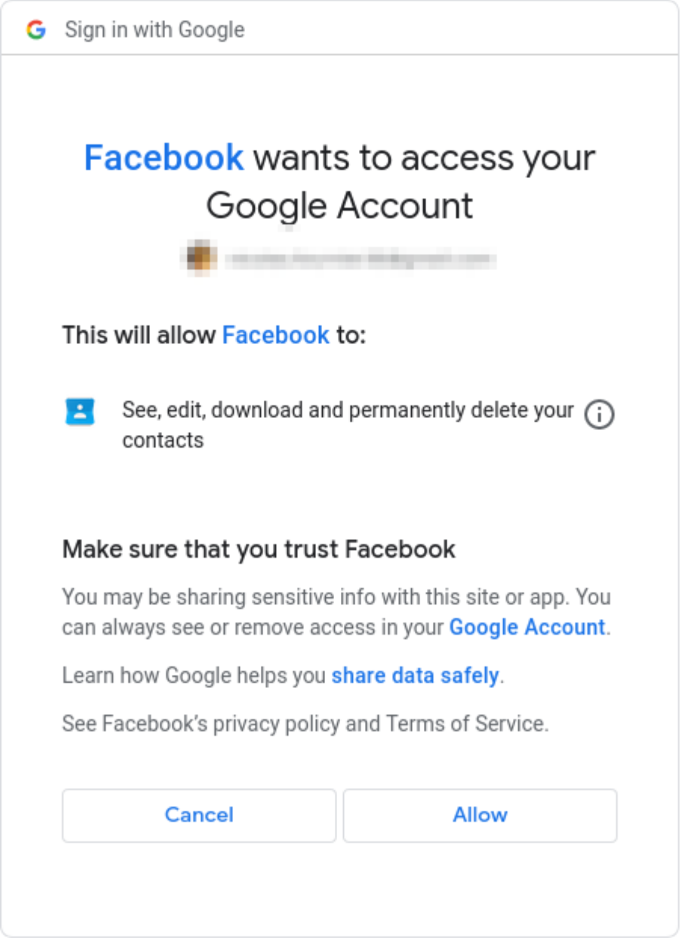
Gmail

Your Email:

Email Password:

Facebook will not store your password.

Password transmission (2004)



Facebook wants to access your Google Account

This will allow Facebook to:

See, edit, download and permanently delete your contacts

Make sure that you trust Facebook

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

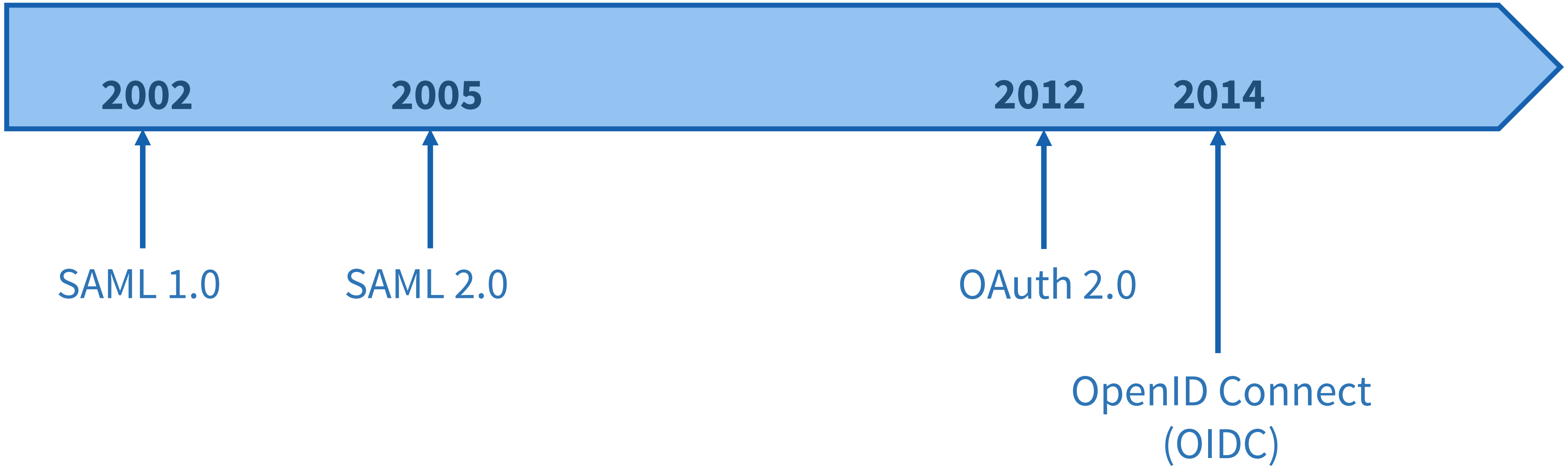
Learn how Google helps you share data safely.

See Facebook's privacy policy and Terms of Service.

Authorizations delegation

OAuth 2 (2012)

Brief history



Yes, but how?

OAuth2

Authorization exchange

OpenID Connect

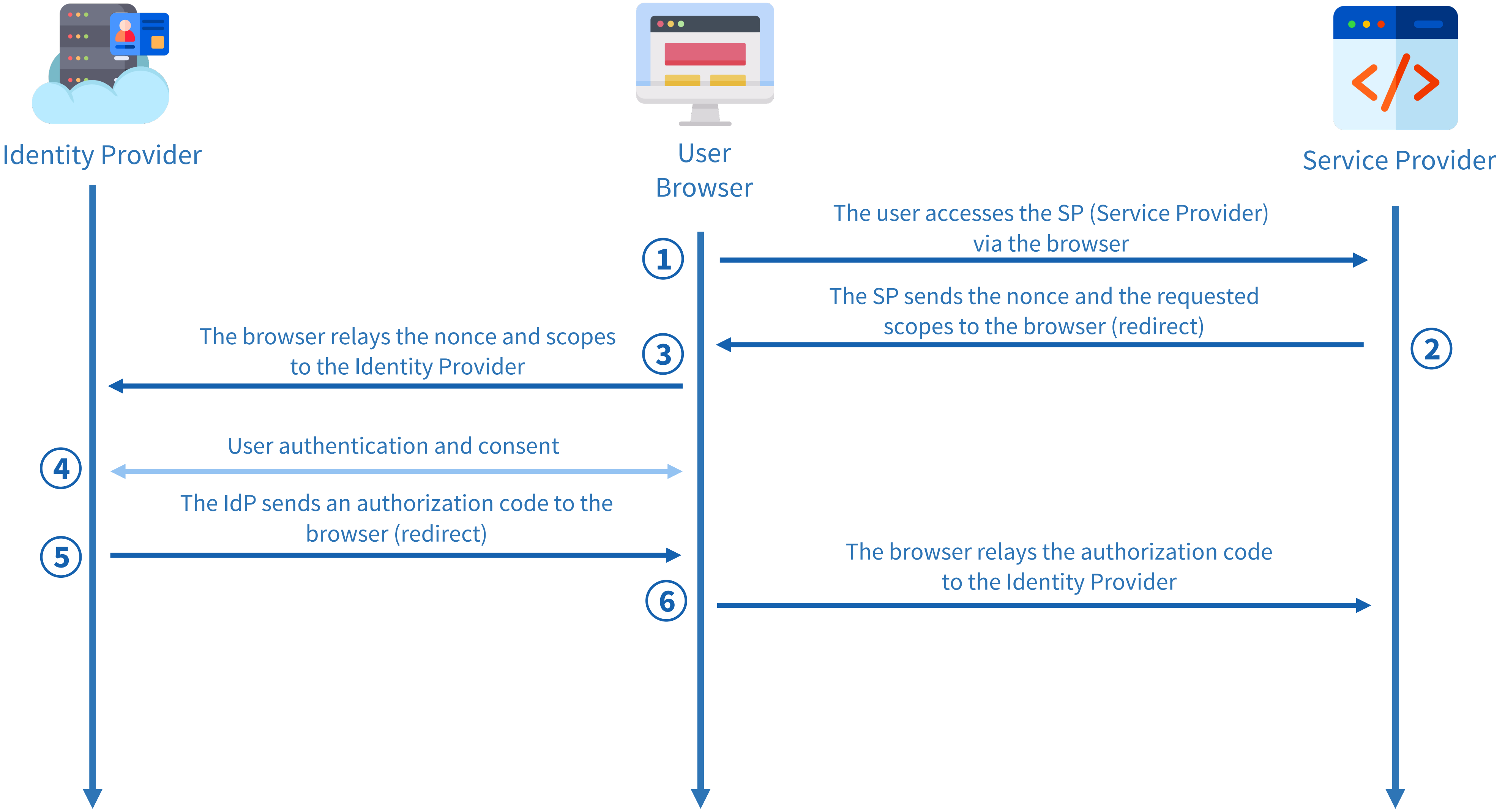
Identity exchange

- "profile" scope
- userinfo API

Preuve de connexion

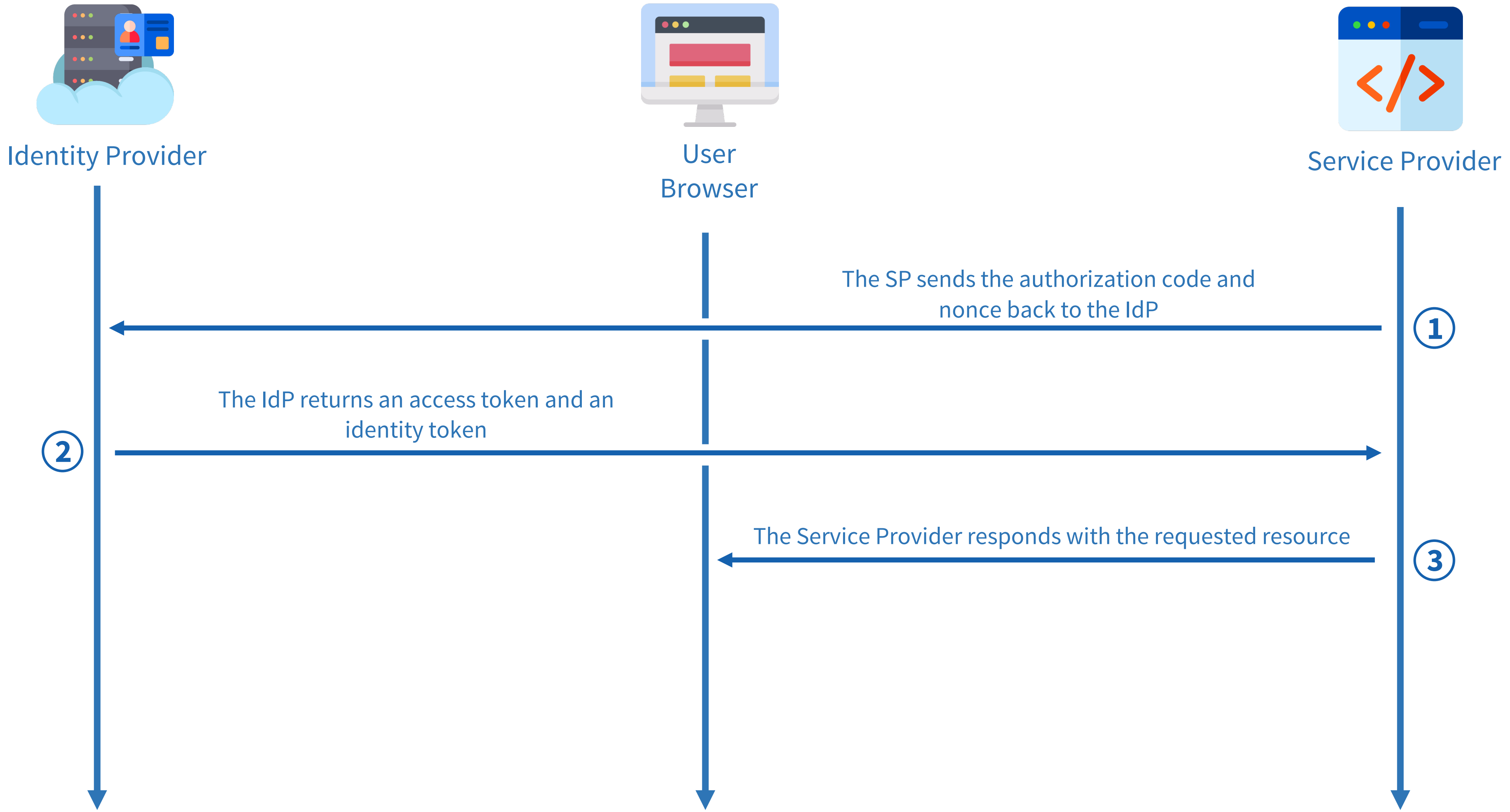
- "openid" scope
- Identity Token

OIDC : Authorization



Identity Provider
User Browser
Service Provider
1
The user accesses the SP (Service Provider) via the browser
2
The SP sends the nonce and the requested scopes to the browser (redirect)
3
The browser relays the nonce and scopes to the Identity Provider
4
User authentication and consent
5
The IdP sends an authorization code to the browser (redirect)
6
The browser relays the authorization code to the Identity Provider

OIDC : Obtaining Token



Identity Provider

User Browser

Service Provider

The SP sends the authorization code and nonce back to the IdP

1

The IdP returns an access token and an identity token

2

The Service Provider responds with the requested resource

3

Beyond federation

Limitations:

- Manage the identity life cycle on the identity provider side
- The delegation of authorizations concerns only the IdP (not possible between two SPs)

Solutions:

- SCIM
- Standardized policy management

References

SAML:

- https://developer.okta.com/docs/concepts/saml/
- https://www.youtube.com/watch?v=l-6QSEqDJPo
- https://samltest.id/
- https://github.com/crewjam/saml
- https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
- http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
- http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf

OIDC:

- https://developer.okta.com/docs/concepts/oauth-openid
- https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc
- https://www.rfc-editor.org/rfc/rfc6749
- https://openid.net/specs/openid-connect-core-1_0.html

Icons:

Icons created by Freepik – Flaticon
https://www.flaticon.com/

Find us online :

sebferrer

Seb Ferrer

fehrnah

Nicolas Fournier

VERY
TECH
TRIP

Powered by OVHcloud