

One identity to federate them all!

Let's talk about Identity and Access Management (IAM)



Identity and Access Management

Did you say IAM?



What I know

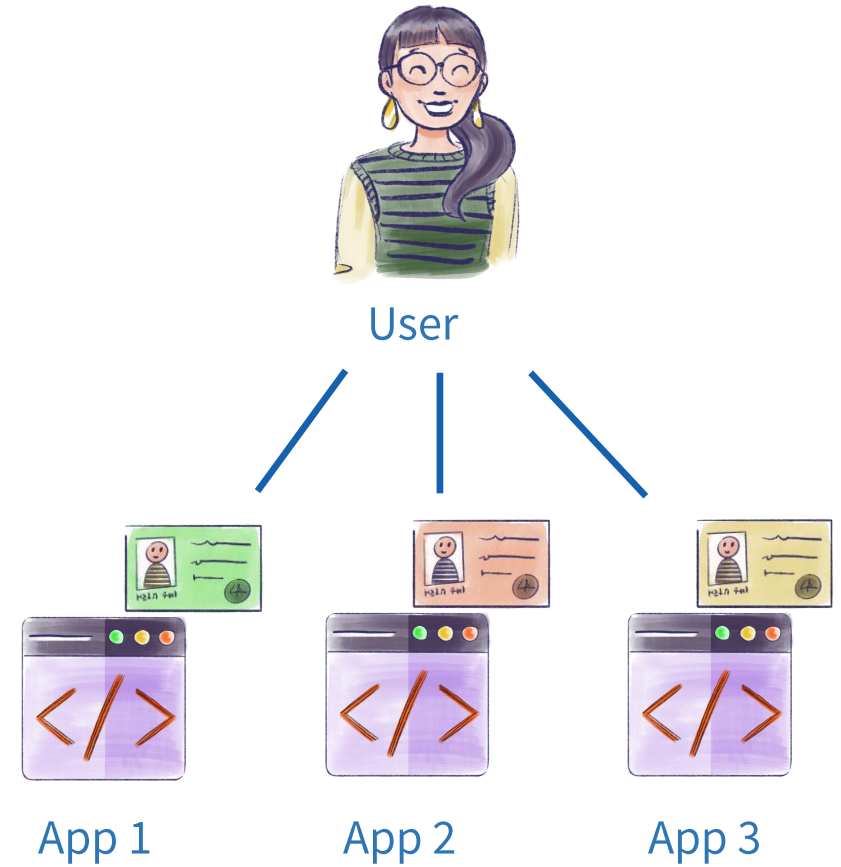
What I have

What I am

Let's talk about authentication

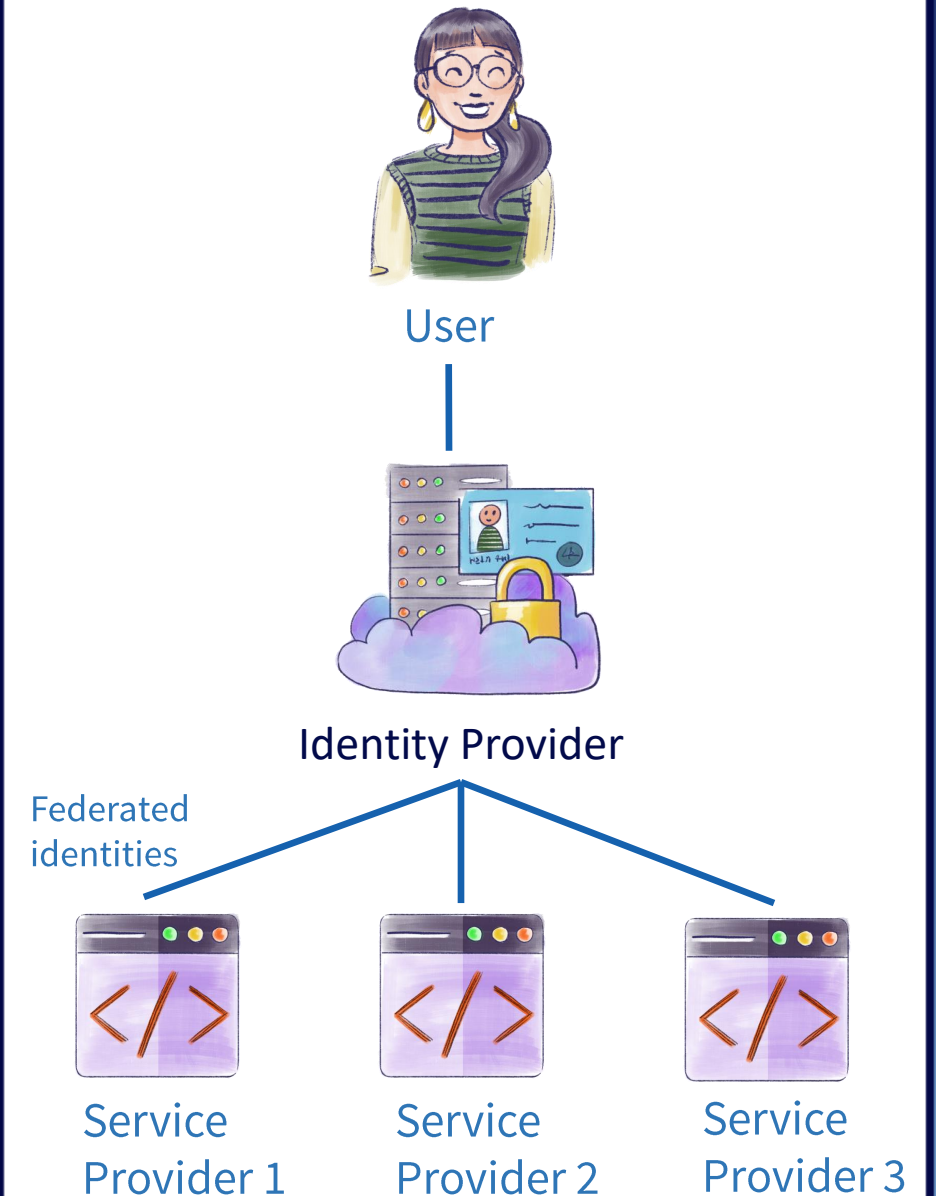
Authentication

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



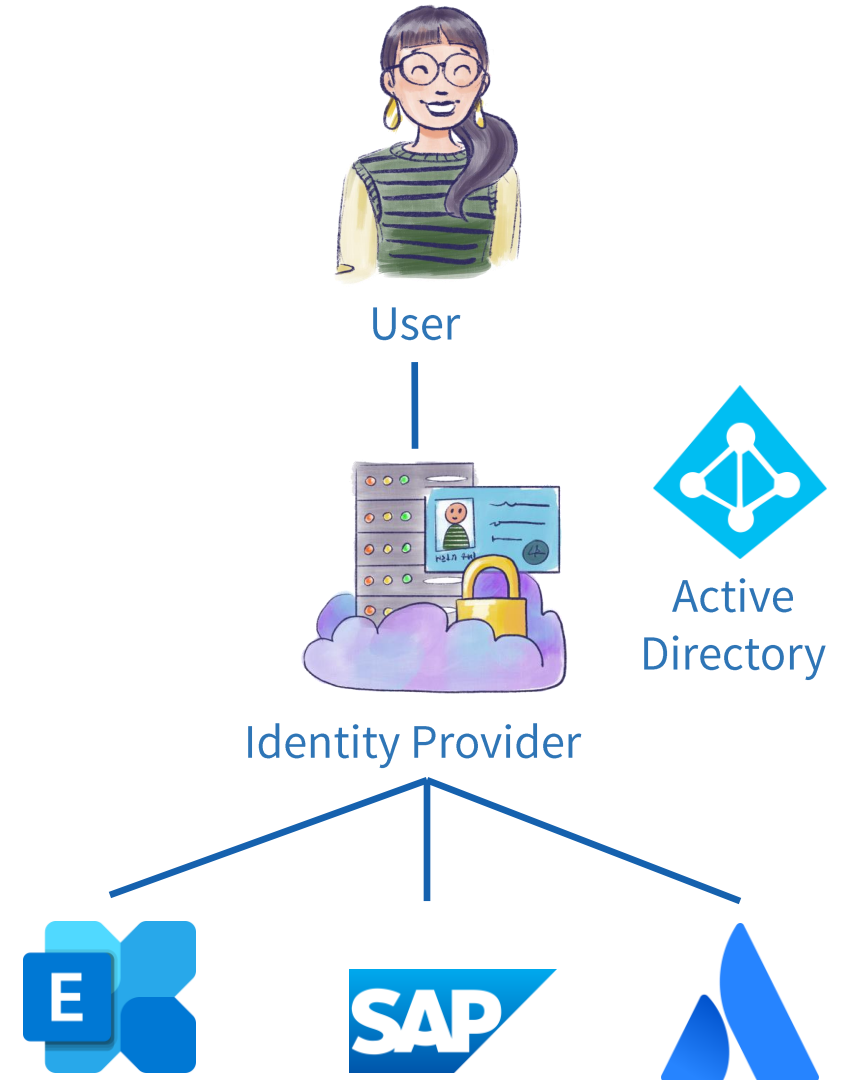
Authentication

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



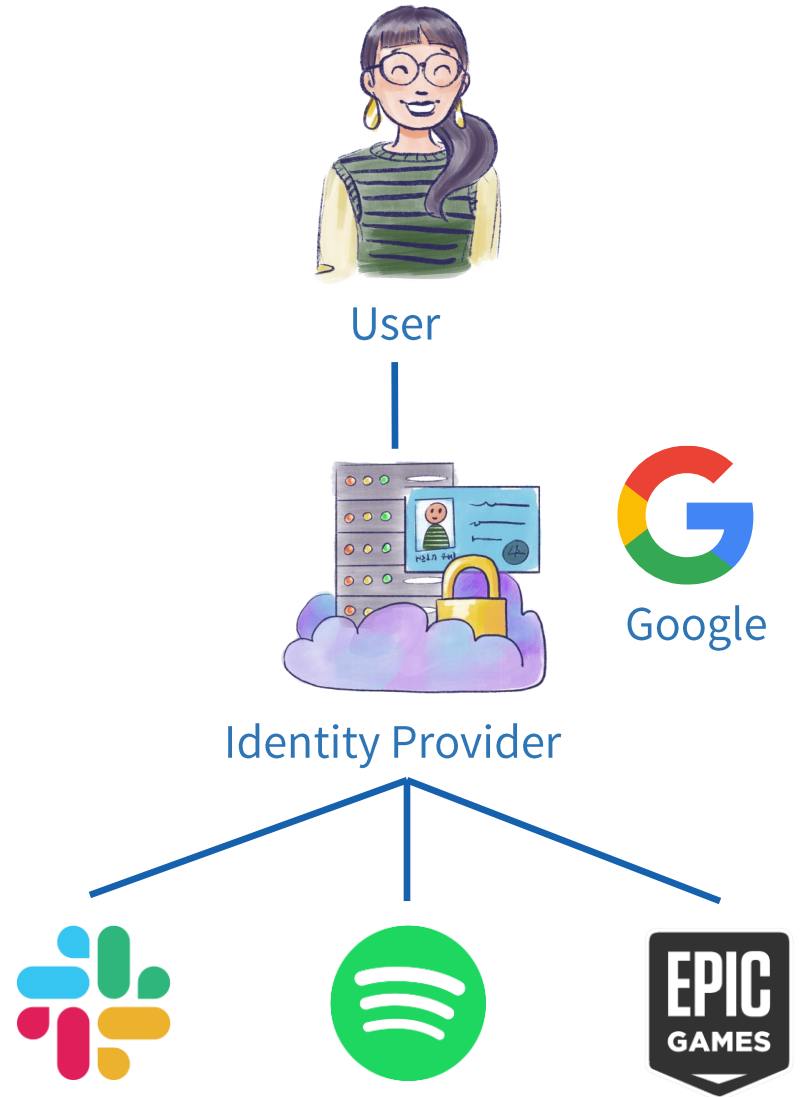
Authentication

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



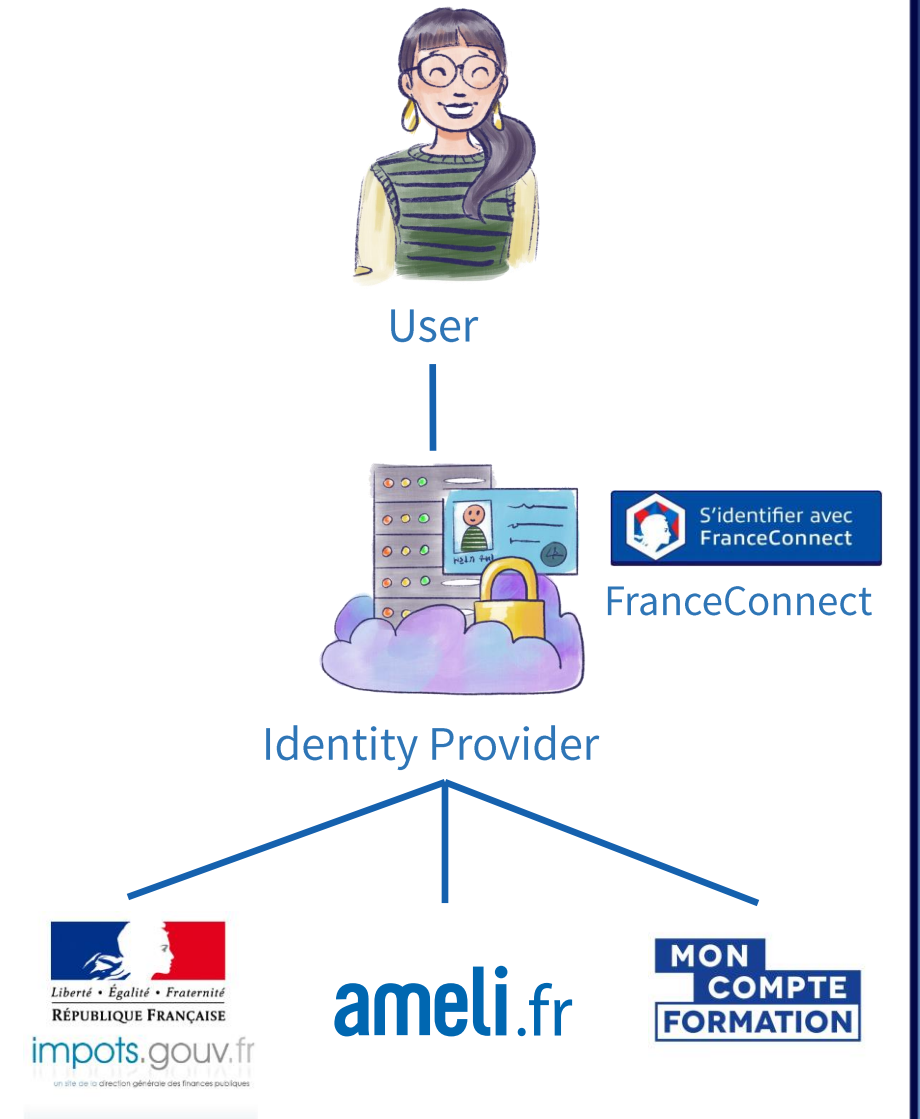
Authentication

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

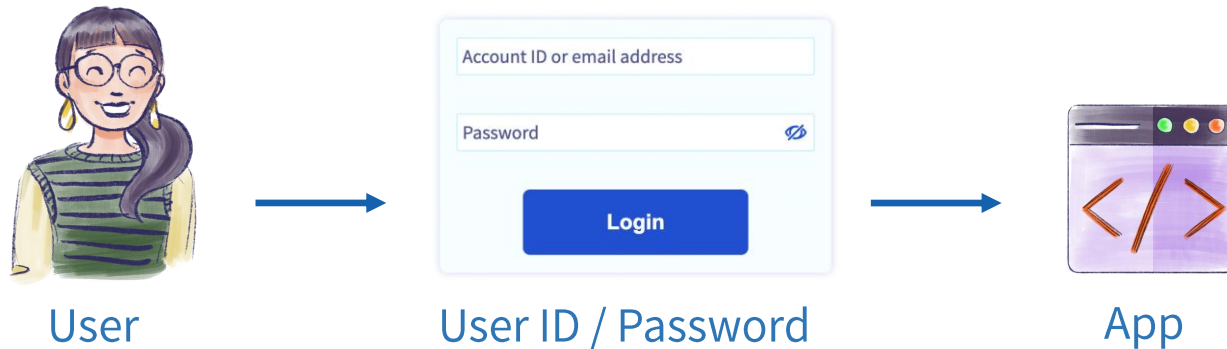


Authentication

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

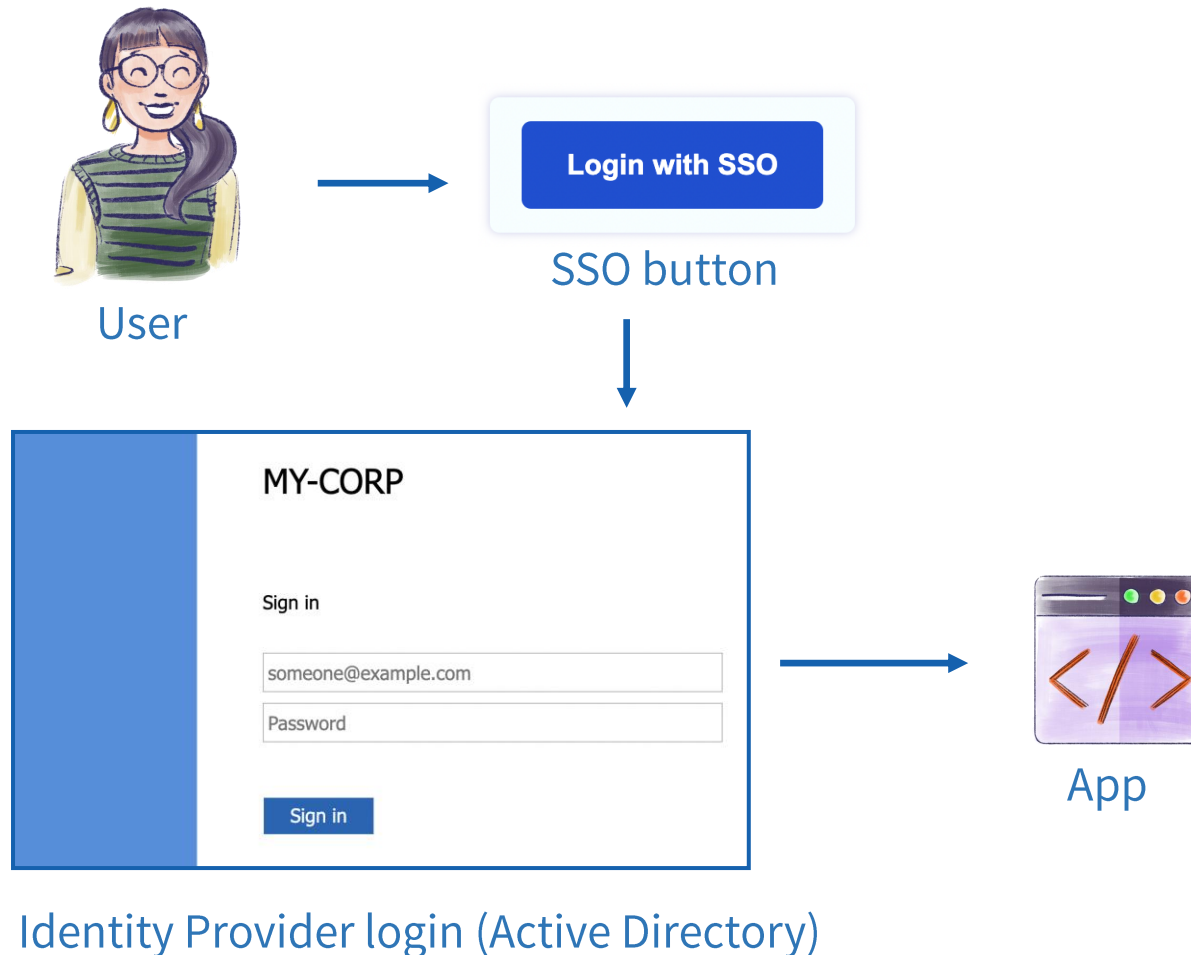


Classic login flow



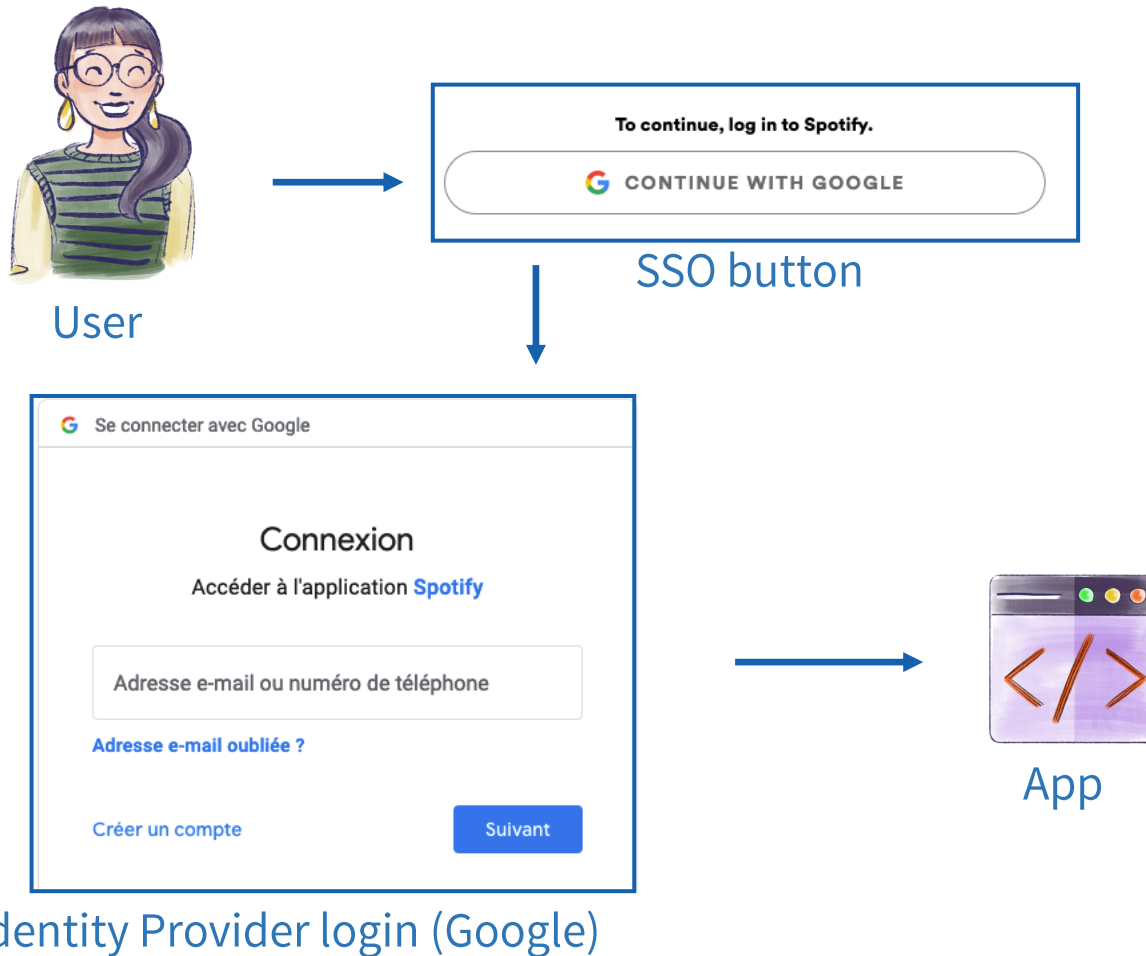
- One identity per application for each user
- App responsible for authentication
- Different login/password per app

Login flow through federation



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

Login flow through federation



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

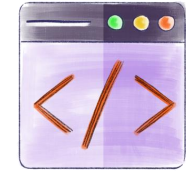
SAML flow



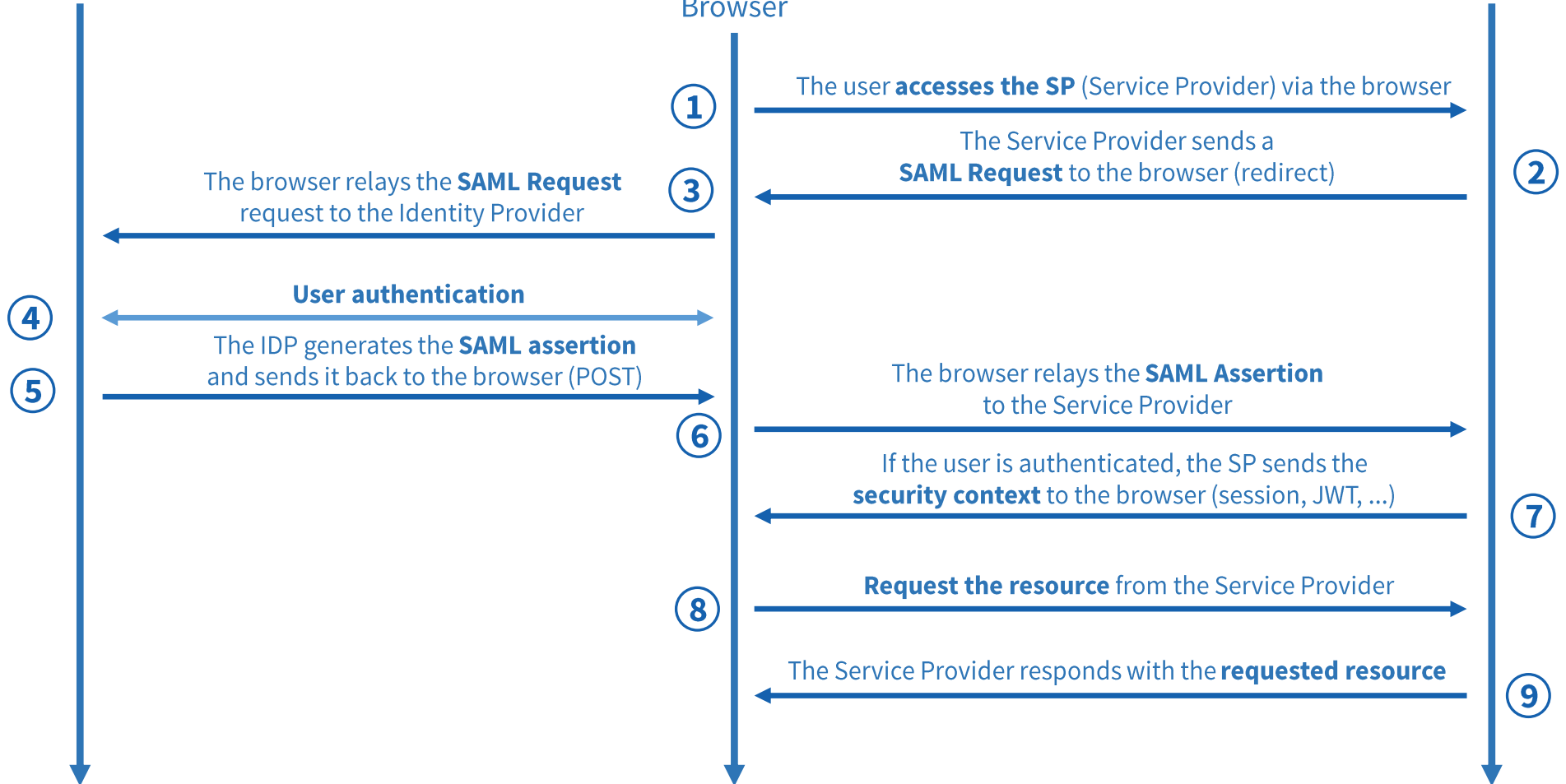
Identity Provider



User
Browser



Service Provider



SAML Trust

Provides to SP:

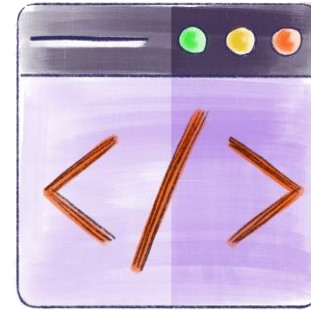


Identity Provider



IdP Metadata file

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



Service Provider

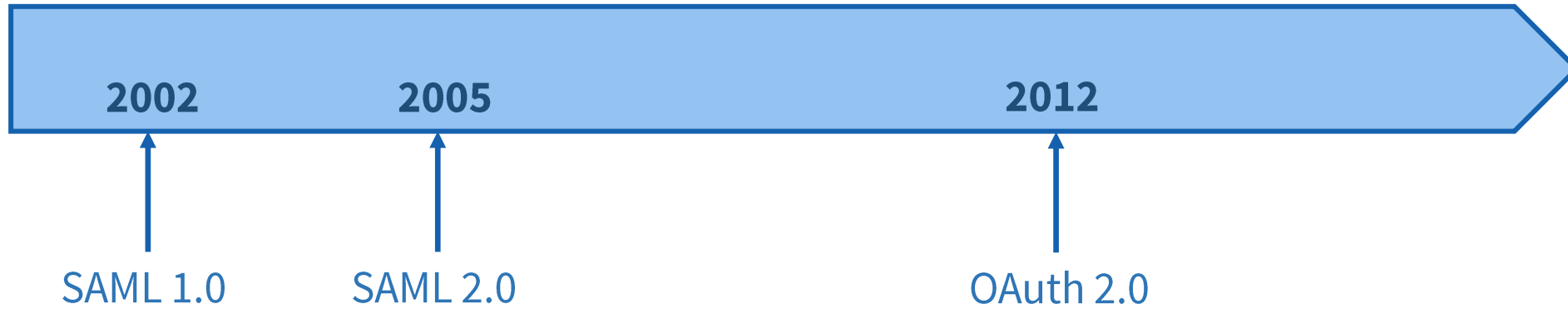
Provides to IdP:



SP Metadata file

- SP Issuer
- SP ACS URL
- SP Certificate

Brief history



OAuth 2


Step 1 Find Friends Step 2 Profile Information Step 3 Profile Picture


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.


 **Yahoo!** Find Friends

 **Windows Live Hotmail** Find Friends


 **Other Email Service** Find Friends

Password transmission
(2004)





 Sign in with Google

Facebook wants to access your
Google Account

 [Redacted Name]

This will allow **Facebook** to:

-  See, edit, download and permanently delete your contacts 

Make sure that you trust Facebook

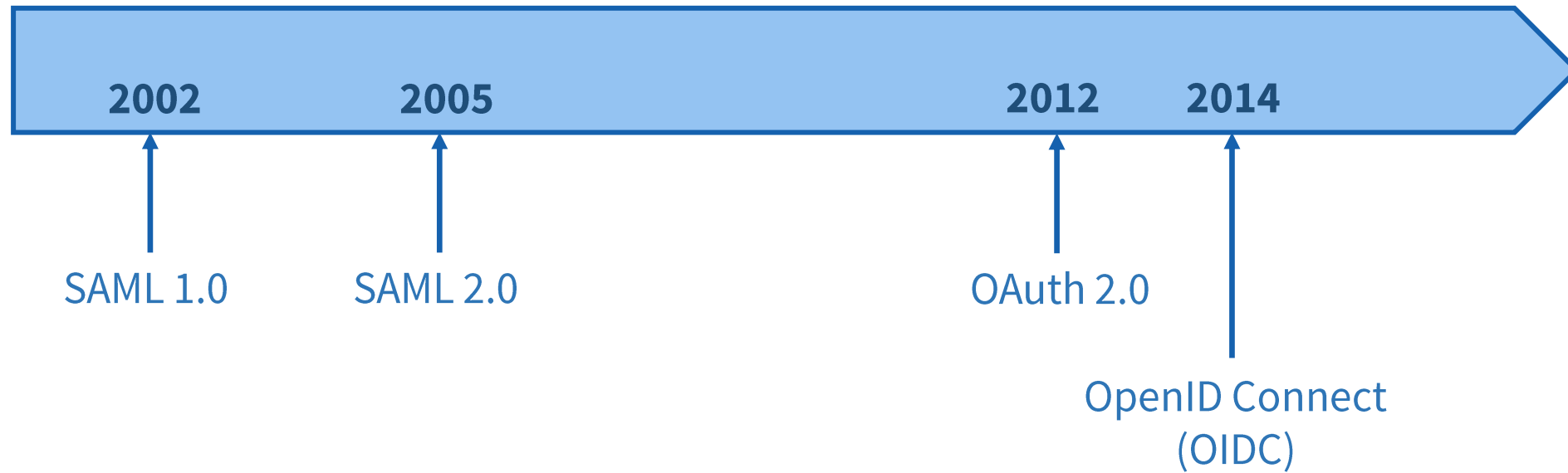
You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See Facebook's privacy policy and Terms of Service.

Authorizations delegation
OAuth 2 (2012)

Birth of OIDC



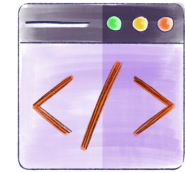
OIDC : Authorization



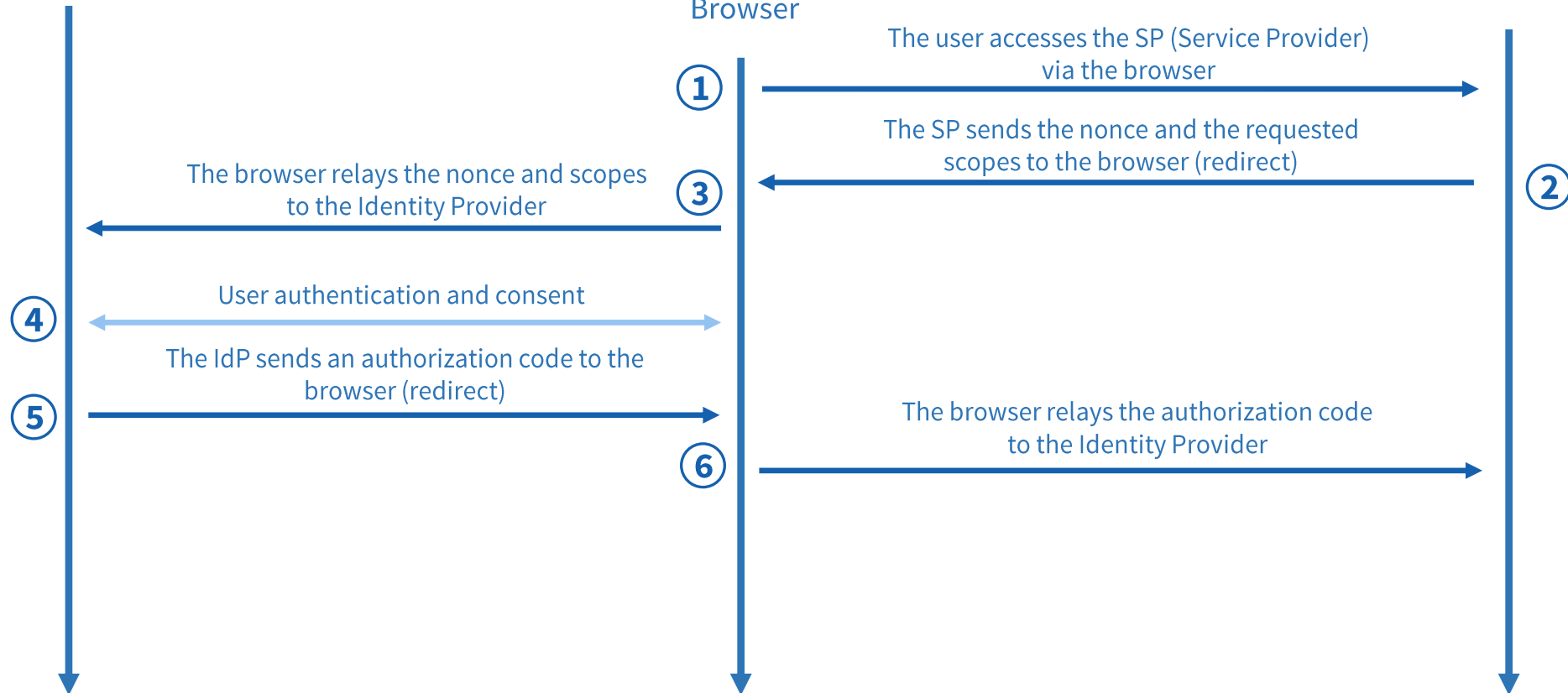
Identity Provider



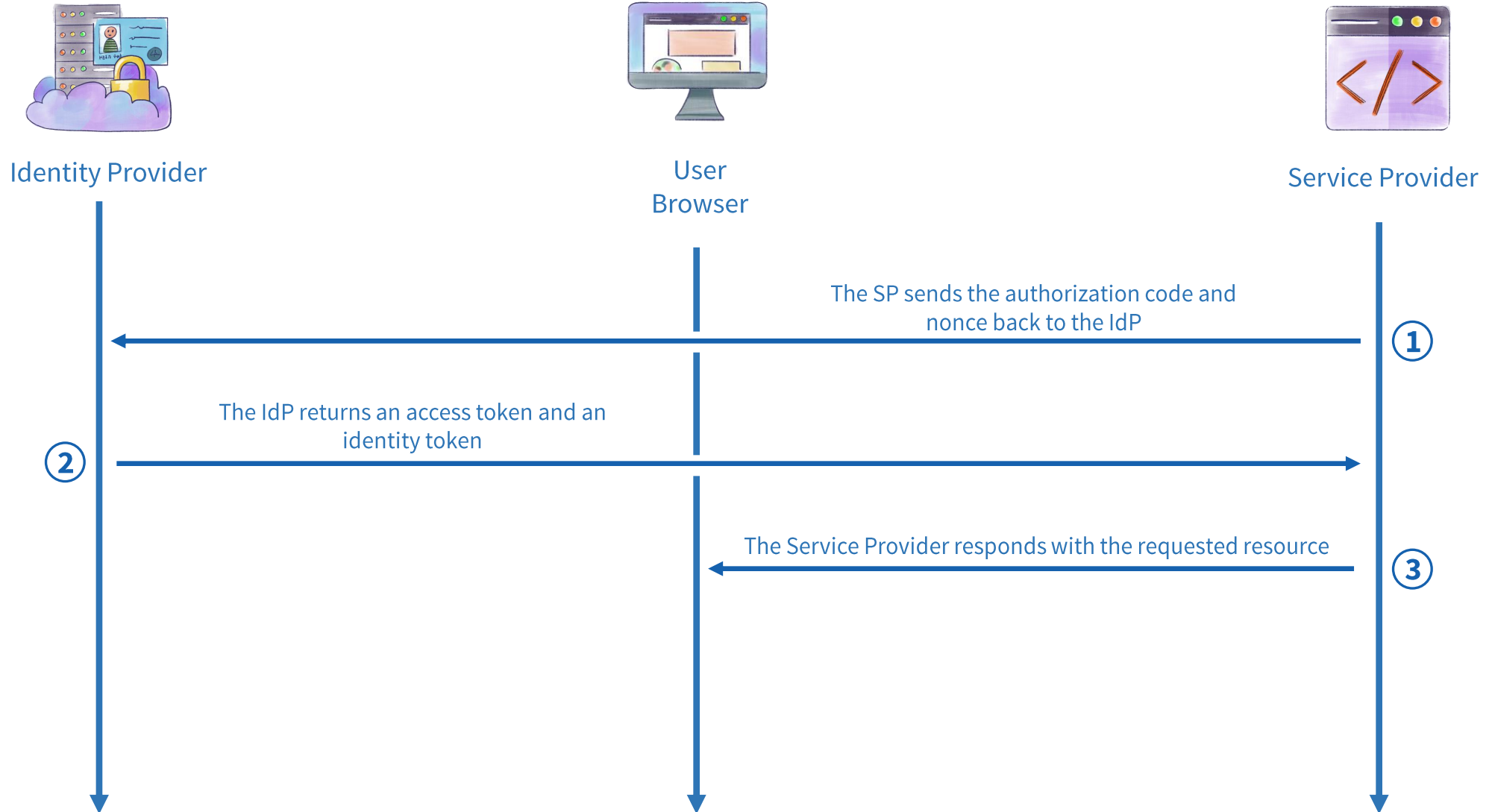
User
Browser



Service Provider



OIDC : Obtaining Token



Beyond federation

Points of attention

- Single point of failure
- Data privacy
- Data compromise

Advices

- Redundancy systems
- Be aware
- MFA

Beyond federation

Limitations

- The delegation of authorizations concerns only the IdP (not possible between two SPs)

Solutions

- Standardized policy management

References

Identity Federation:

- <https://www.okta.com/identity-101/why-your-company-needs-an-identity-provider/>
- <https://www.okta.com/blog/2022/08/exploration-of-open-identity-standards/>
- <https://www.descope.com/blog/post/saml-vs-oidc>
- <https://securityintelligence.com/posts/identity-and-access-management-evolution/>

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

References

SAML:

- <https://developer.okta.com/docs/concepts/saml/>
- <https://blog.thibz.xyz/p/everything-you-should-know-about-saml-and-how-to-exploit-it/>
- <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>

Icons:

Freepik – Flaticon

<https://www.flaticon.com/>

elissakarminakria (Instagram)

Find me online :



sebferrer



seb-ferrer



<https://blog.kimi.ovh>