Fédérez-vous !

Une plongée dans le monde merveilleux de la gestion des accès

Bastien Huber

Bastien Huber

centralelille

Promo 2017

extia

2018

Mission à l'Imprimerie Nationale

Plan

I. Introduction à l'*Identity and Access Management (IAM)*
II. Fédérer les identités
III. Gérer les authentifications

Identity and Access Management

Les 3 composantes de l'IAM

Identité

Unique
Non-prédictive
Permanente
Simple

Authentification

Ce que je *suis*
Ce que je *sais*
Ce que *j'ai*

Autorisation

Gros grains (*coarse grained)*
Grains fins (*fined grained)*

Identity and Access Management

Pour quoi ?






DON’T PANIC

Utilisateur·ices :

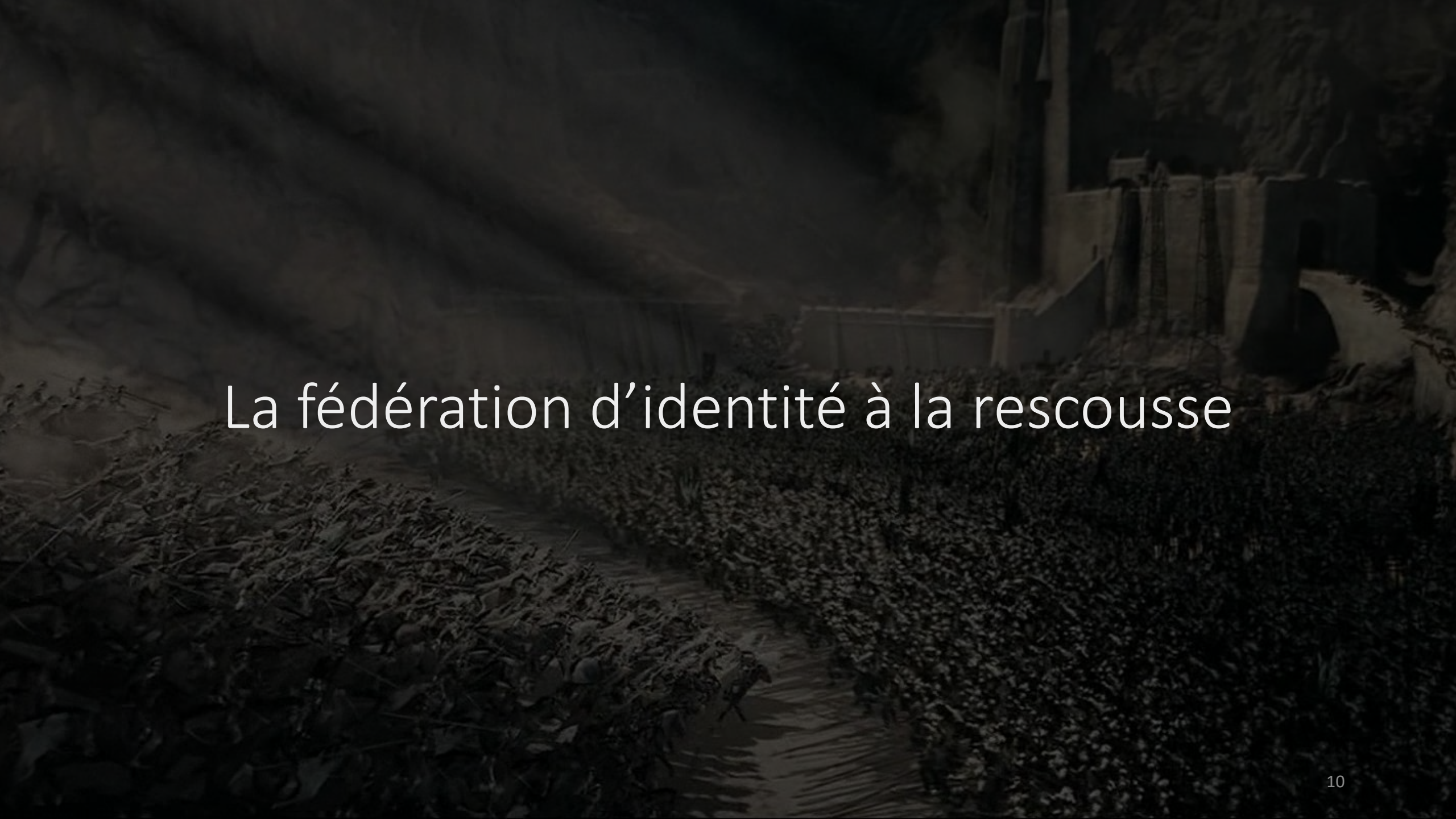
- Plein d’identités et de mots de passe à gérer
- Temps de perdu à chaque connexion
- Faire des demandes d’accès pour chaque ressource
- Dépendance envers la DSI

DSI

- Gestion du cycle de vie des identités
- Gérer le nombre de licences à fournir
- Gérer les appels et demandes d’accès

RSSI et Service Juridique

- Savoir qui a accès à quoi ?
- RGPD
- Limiter le *Shadow IT*



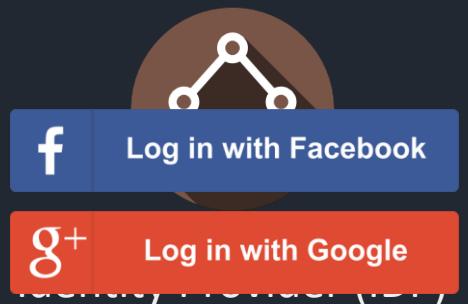
La fédération d’identité à la rescousse

Fédération d’identité

Utiliser une identité unique pour s’authentifier
sur de multiples services

Fédération d’identité

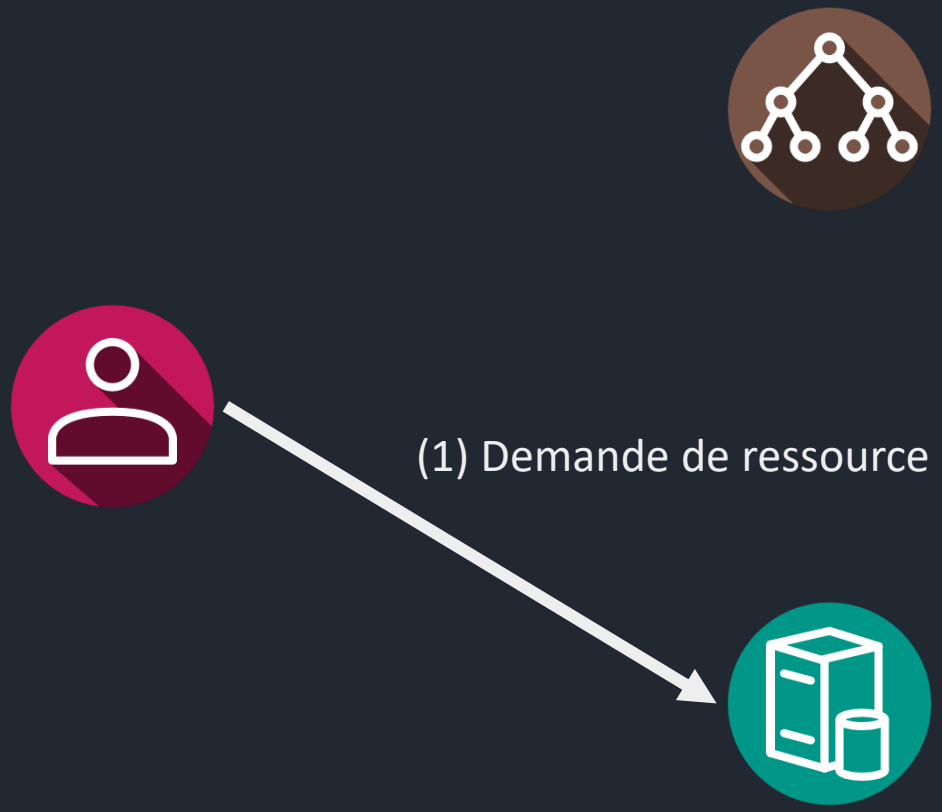
Réseaux sociaux



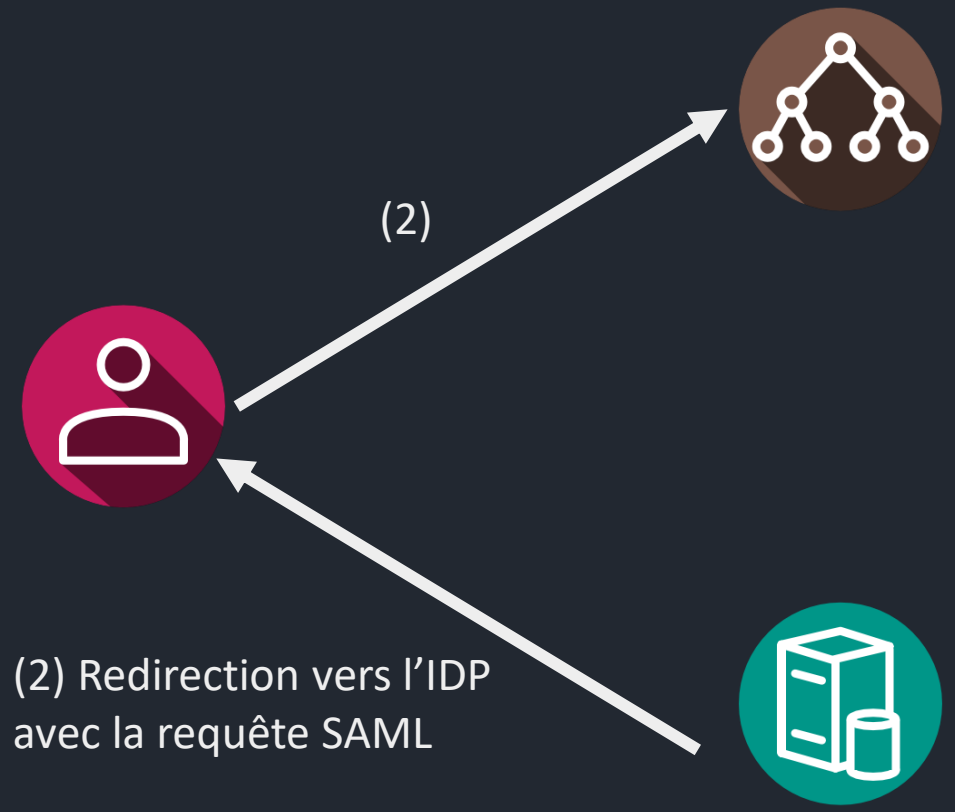
Applications de Single Sign-On

Service Provider (SP)

Fédération d’identité : SAML 2

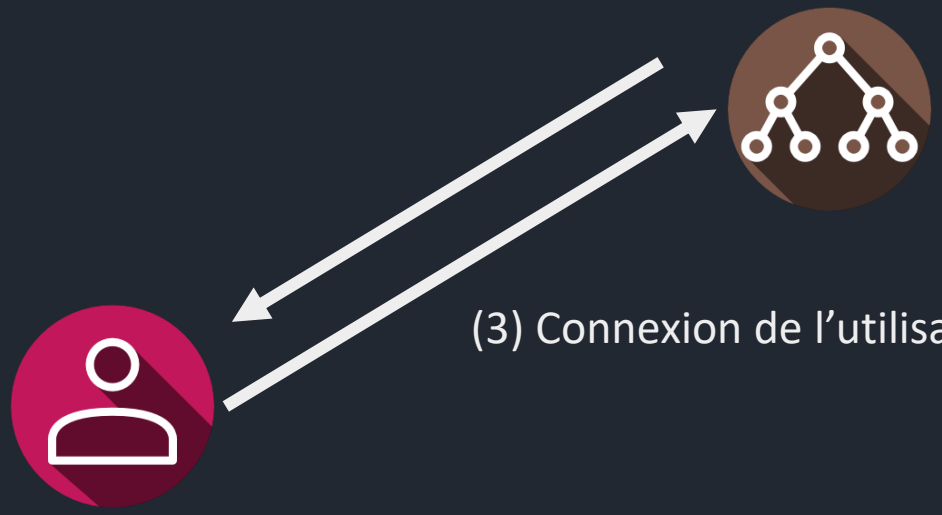


Fédération d’identité : SAML 2



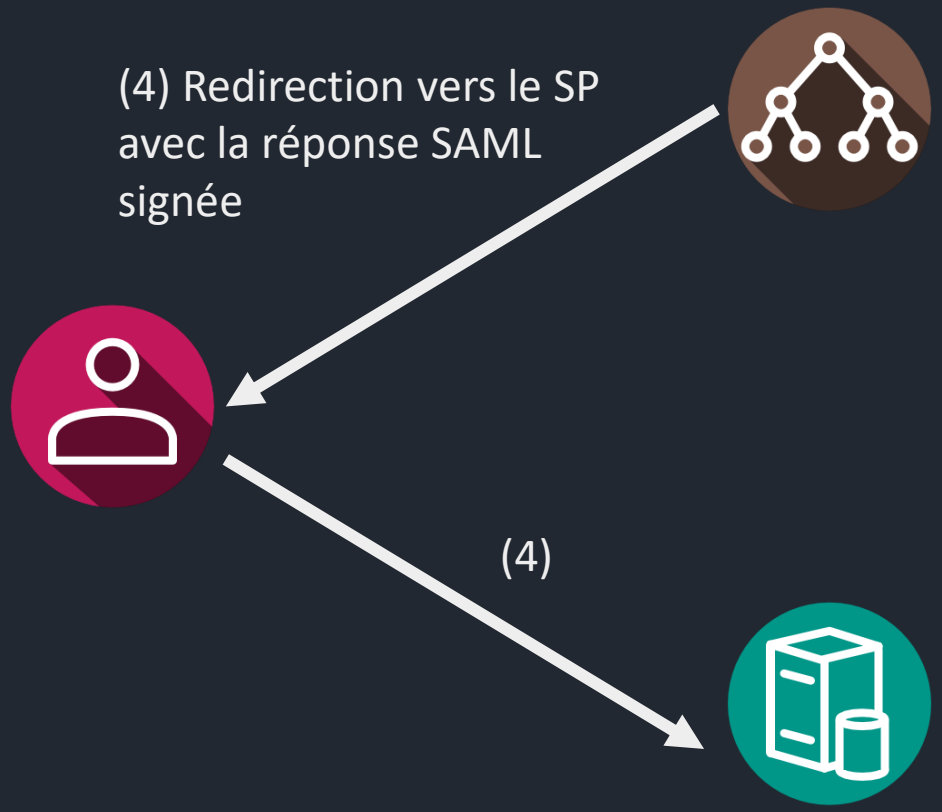

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2018-12-08T11:40:00Z"
  AssertionConsumerServiceIndex="0"
  AttributeConsumingServiceIndex="0">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
  <samlp:NameIDPolicy
    AllowCreate="true"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
</samlp:AuthnRequest>
```

Fédération d’identité : SAML 2



(3) Connexion de l’utilisateur à l’IDP

Fédération d’identité : SAML 2




```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="identifier_2"
  InResponseTo="aaf23196-1773-2113-474a-fe114412ab72 "
  Version="2.0"
  IssueInstant="2004-12-05T09:22:05Z"
  Destination="https://sp.example.com/SAML2/SSO/POST">
  <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
    <samlp:Status>
    <samlp:StatusCode
    Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="identifier_3"
    Version="2.0"
    IssueInstant="2004-12-05T09:22:05Z">
    <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
    <ds:Signature
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
        3f7b3dcf-1674-4ecd-92c8-1544f346baf8
      </saml:NameID>
      <saml:SubjectConfirmation
        Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
          InResponseTo="identifier_1"
          Recipient="https://sp.example.com/SAML2/SSO/POST"
          NotOnOrAfter="2004-12-05T09:27:05Z"/>
      </saml:SubjectConfirmation>
```

Fédération d’identité : SAML 2

Les limites

- Verbeux
- Peu adapté au fonctionnement des API
- Pas adapté au fonctionnement d’applications mobiles
- Pas de délégation d’autorisation
- HTTPS pas obligatoire


OAUTH
2
OAUTH

OAuth 2.0

Resource Owner

Authorization Server

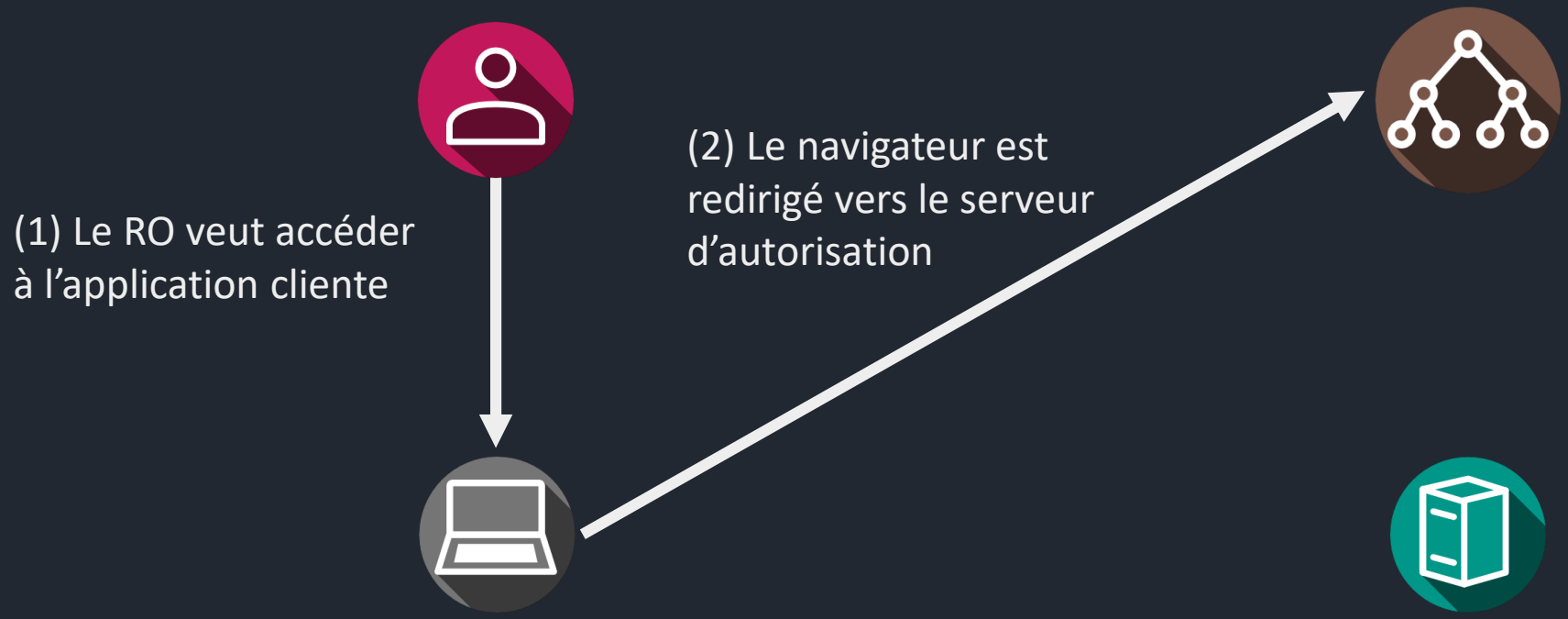
Client

Resource server

OAuth 2.0

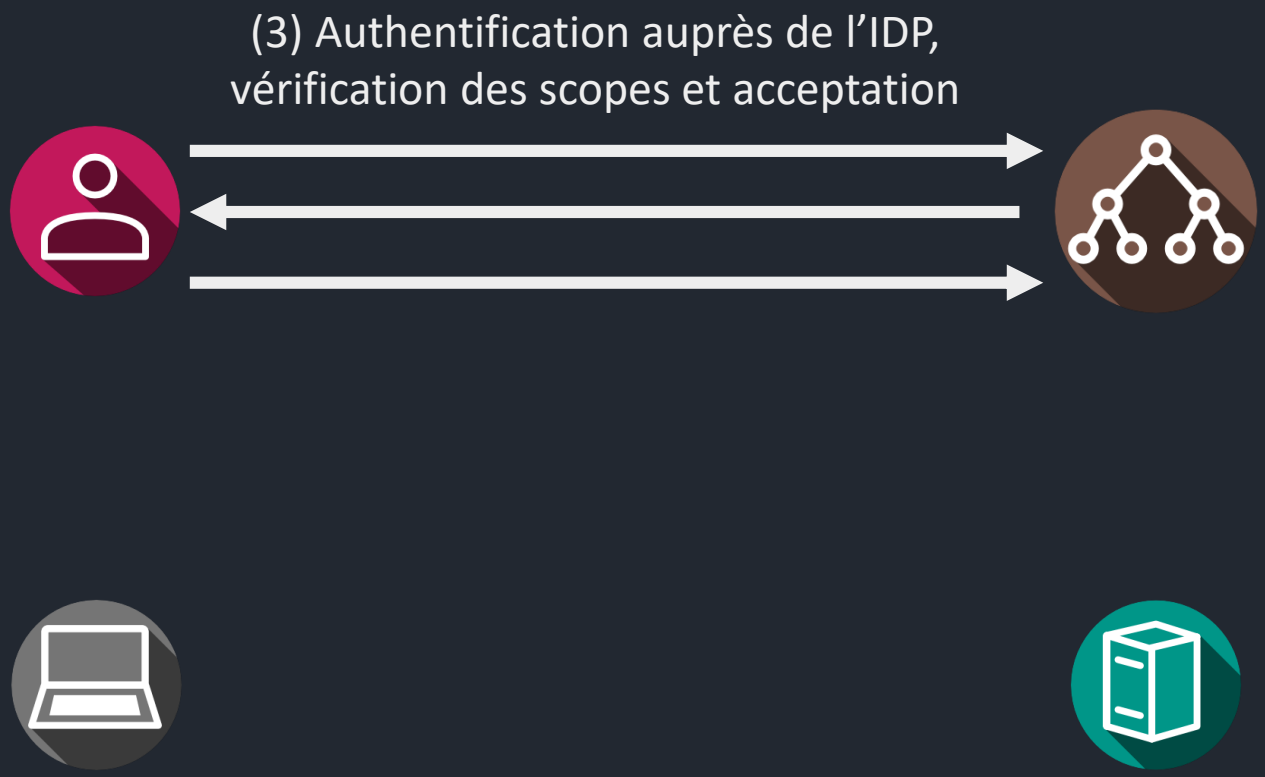
Authorization Code Grant

https://github.com/login?client_id=bbe1fe17fd3206756805&redirect_uri=https%3A%2F%2Fgitlab.com%2Fusers%2Fauth%2Fgithub%2Fcallback&response_type=code&scope=user%3Aemail&state=dbec4bb41de0d58928ea24c52c48130a0155489dcee07927



OAuth 2.0

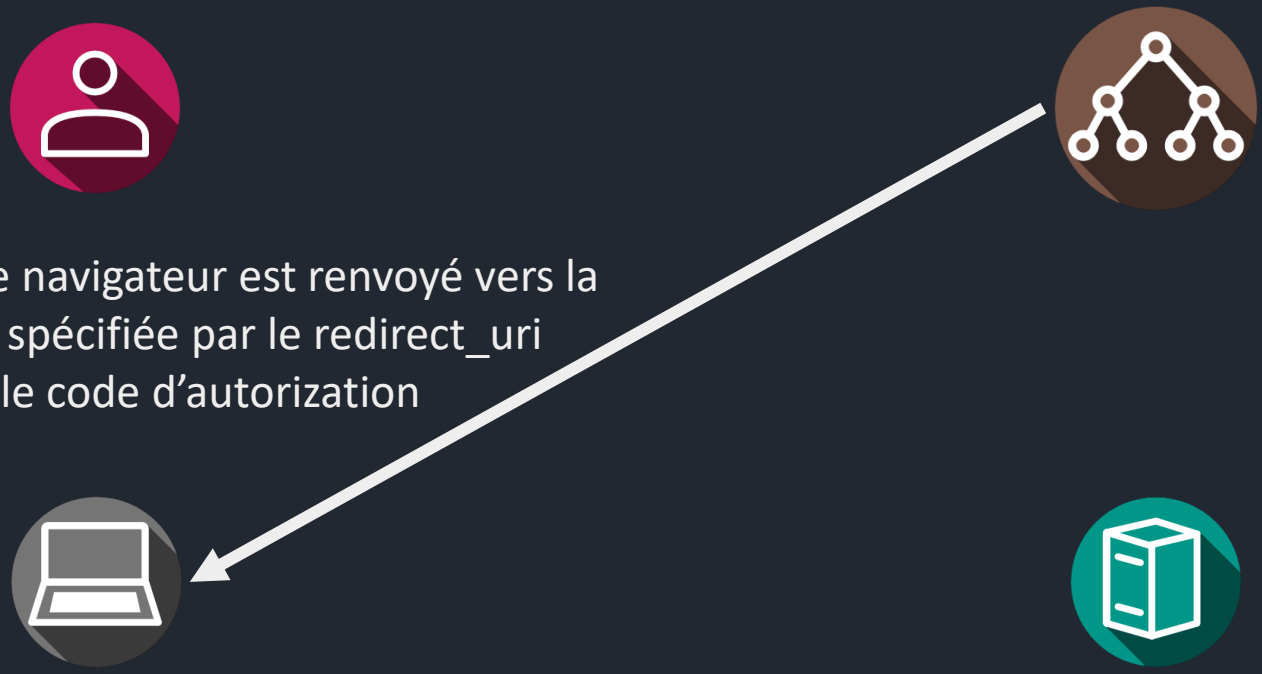
Authorization Code Grant



OAuth 2.0

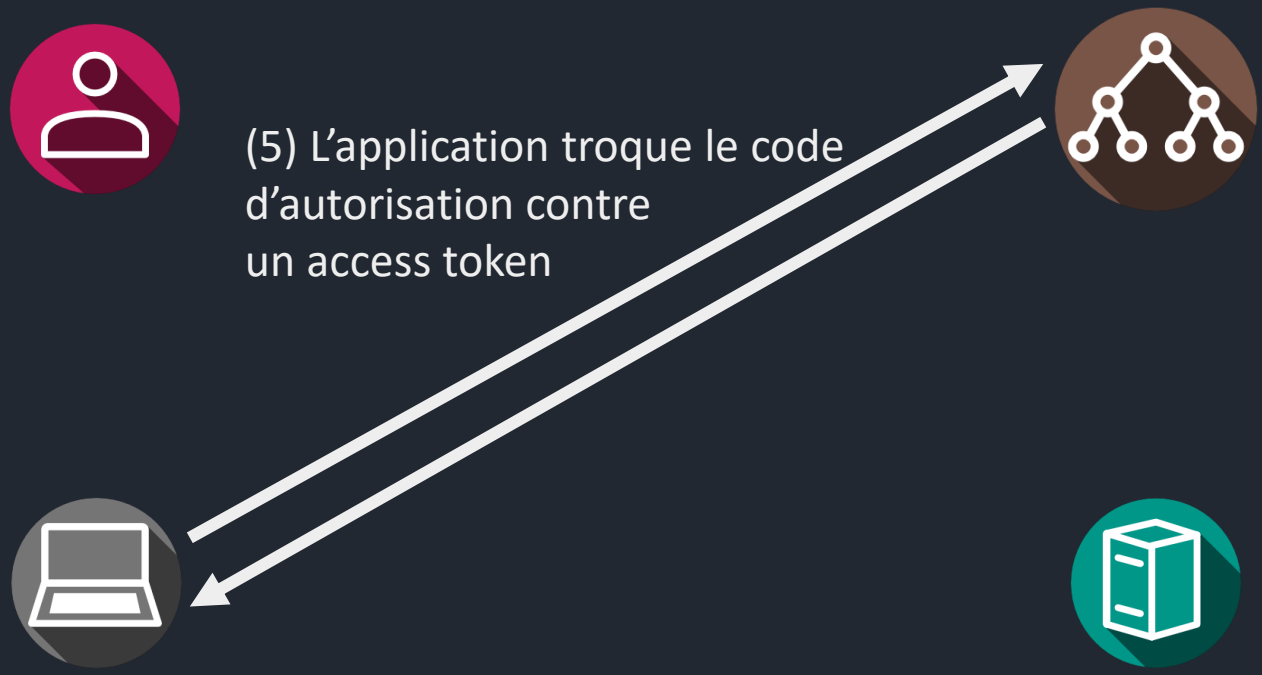
Authorization Code Grant

https://gitlab.com/users/auth/github/callback?code=rACJhwYjgsCCRhyAtDzfcFqXmP2eYJxl_a6wUUzuOPq7e99Ftt0ICNfHRzhbN2J0BECrCwytyN3V3ObcqSIVj68&scope=user%3Aemai&session_state=64f20e685fd850f7dc3867b4d2b0dbcc1fae4b07



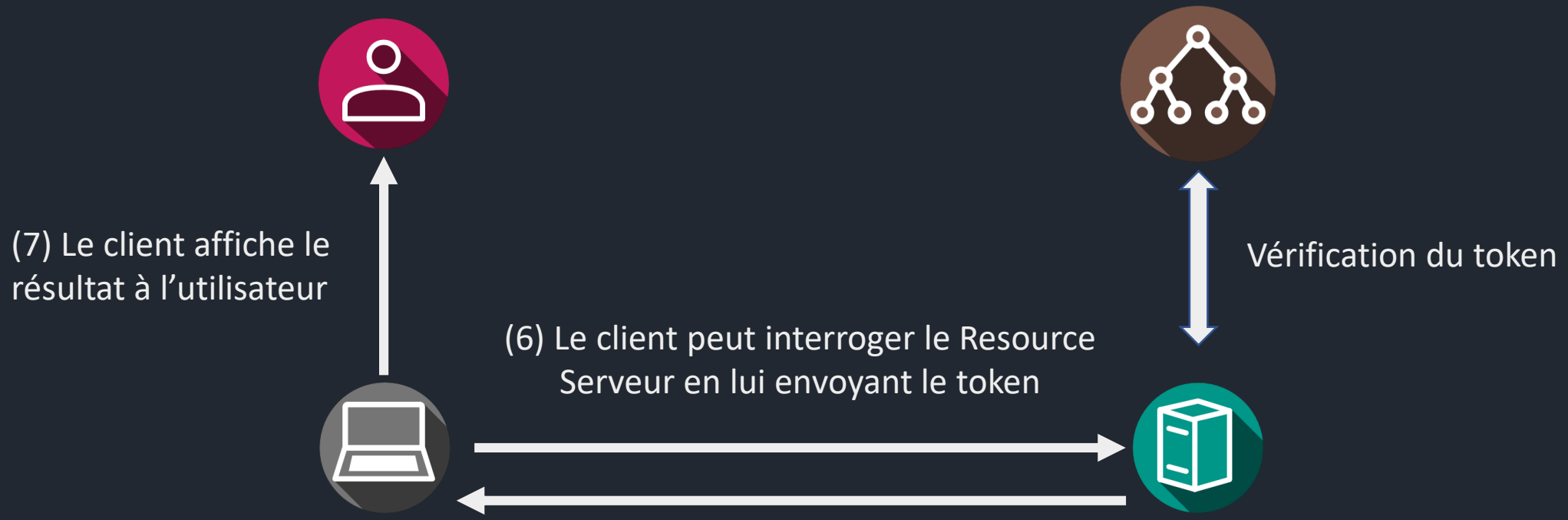
OAuth 2.0

Authorization Code Grant



OAuth 2.0

Authorization Code Grant



OAuth 2.0

Les différents flux

Client Credential	Authorization Code	Resource Owner Password Credentials	Implicit
Si l'application cliente est le RO	Web app côté serveur ou app mobile	Si on fait confiance au client pour gérer les credentials	SPA & Mobile app Plus utilisé, à la place Authorization Code PKCE

OAuth 2.0

Avantages par rapport à SAML v2

- HTTPS obligatoire
- Moins verbeux
- Délégation d’autorisation
- On peut (théoriquement) choisir les données à partager

OAuth 2.0

Inconvénients

- Plus d’appels à réaliser
- Le client n’a pas directement d’infos sur l’utilisateur

OpenID Connect

OpenID Connect

- Surcouche d’identification à Oauth 2.0
- « ID Token » (JWT) en plus de « l’Access Token »
- UserInfo Endpoint

- Pas d’instructions sur la manière dont l’authentification doit être réalisée

Méthodes d’authentification

Méthodes d’authentification

Mot de passe

Passphrase Question

Code PIN

Reconnaissance Faciale

Empreintes digitales

Reconnaissance vocale Rétine

OTP Code reçu par mail/sms Carte d’identité

FIDO2 Challenge signé Passeport

Notification à accepter sur téléphone Token physique

En résumé

- L’IAM simplifie la vie de tout le monde…
- Sauf de celui ou celle qui doit la mettre en place
- Permet de veiller à la sécurisation du SI
- S’appuie sur des standards (SAML, OAuth, FIDO…)

Sources

- https://blog.octo.com/utiliser-la-federation-d%E2%80%99identite-sur-votre-site-web/
- https://en.wikipedia.org/wiki/SAML_2.0
- https://www.gluu.org/blog/oauth-vs-saml-vs-openid-connect/
- https://nordicapis.com/api-security-oauth-openid-connect-depth/
- https://www.oauth.com/oauth2-servers/pkce/authorization-code-exchange/