Mécanismes d'authentification

État de l'art

Matthieu Nicolas

20/09/2016

Plan

Plan

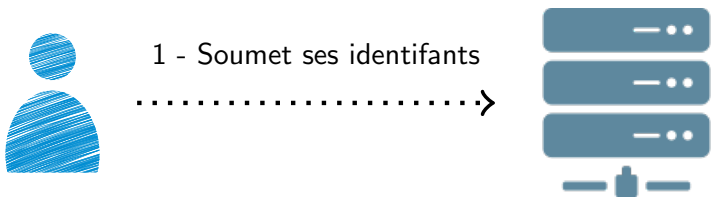
Authentification locale

Principe

- Architecture la plus *intuitive*
- Propose son propre système d'authentification

- Utilise généralement nom d'utilisateur/mot de passe
- Possible d'ajouter d'autres facteurs d'authentification
  - Code d'accès
  - Jeton d'authentification

Architecture



Application

Base de données

Architecture

Application

Base de données

Architecture

Application

Base de données

Authentification locale

Avantages vs Inconvénients

- Avantages
  - Solution relativement *simple*
  - Maîtrise de l'environnement
  - Confidentialité

Authentification locale

Avantages vs Inconvénients

- Avantages
  - Solution relativement *simple*
  - Maîtrise de l'environnement
  - Confidentialité
- Inconvénients
  - *Simple* de faire des erreurs
  - Pas de distinction entre le service *métier* et le service *d'authentification*
  - Un compte supplémentaire pour l'utilisateur...

Authentification locale

Bonnes pratiques

HTTPS

- Chiffre les échanges entre le client et le serveur
- Prémunit des attaques *man-in-the-middle*

Chiffrer le mot de passe

- Ne pas stocker le mot de passe en clair
- Utiliser des méthodes *lentes*
  - Bcrypt
  - PBKDF2

Authentification locale

Bonnes pratiques - suite

Ajouter un sel

- Chaîne de caractères aléatoires
- Différente pour chaque utilisateur
- Protège de
  - Attaques par dictionnaire
  - Rainbow table

Authentification locale

Frameworks & Librairies

- Available at `https://plm.telecomnancy.univ-lorraine.fr`

Plan

Authentification déléguée

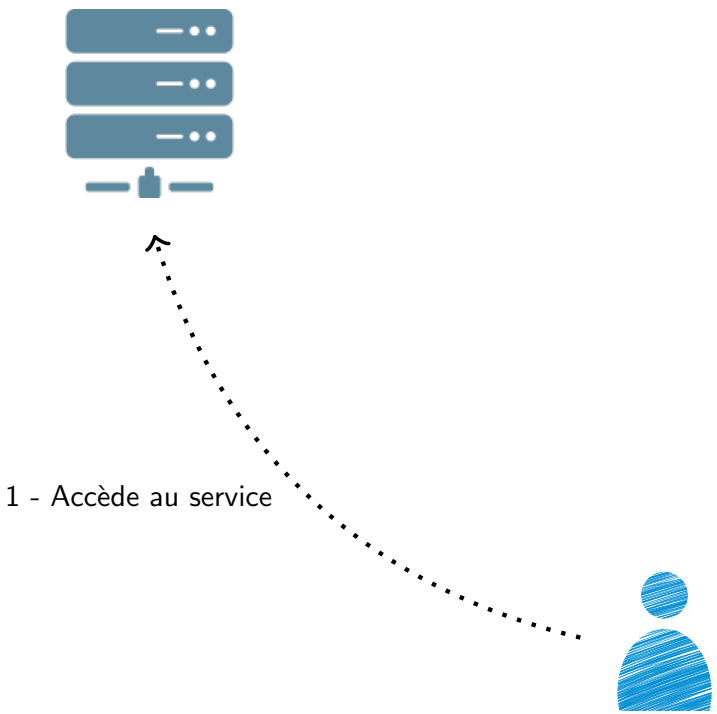
Principe

- Sépare le rôle des différents composants :
  - **Fournisseur d'identité (Identity Provider)**
  - **Fournisseur de service (Service Provider)**
- Pour pouvoir utiliser le service, l'utilisateur doit fournir une preuve de son identité
- Un seul service peut être compatible avec plusieurs fournisseurs d'identité
- Un seul compte permet de s'authentifier auprès de plusieurs services (**Single Sign-On : SSO**)

Architecture

Fournisseur de service

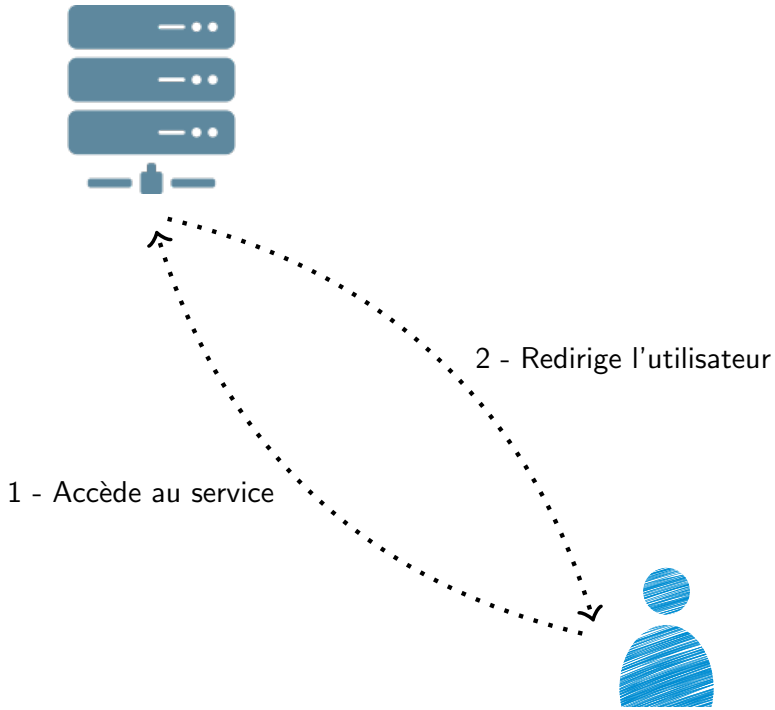
Fournisseur d'identité



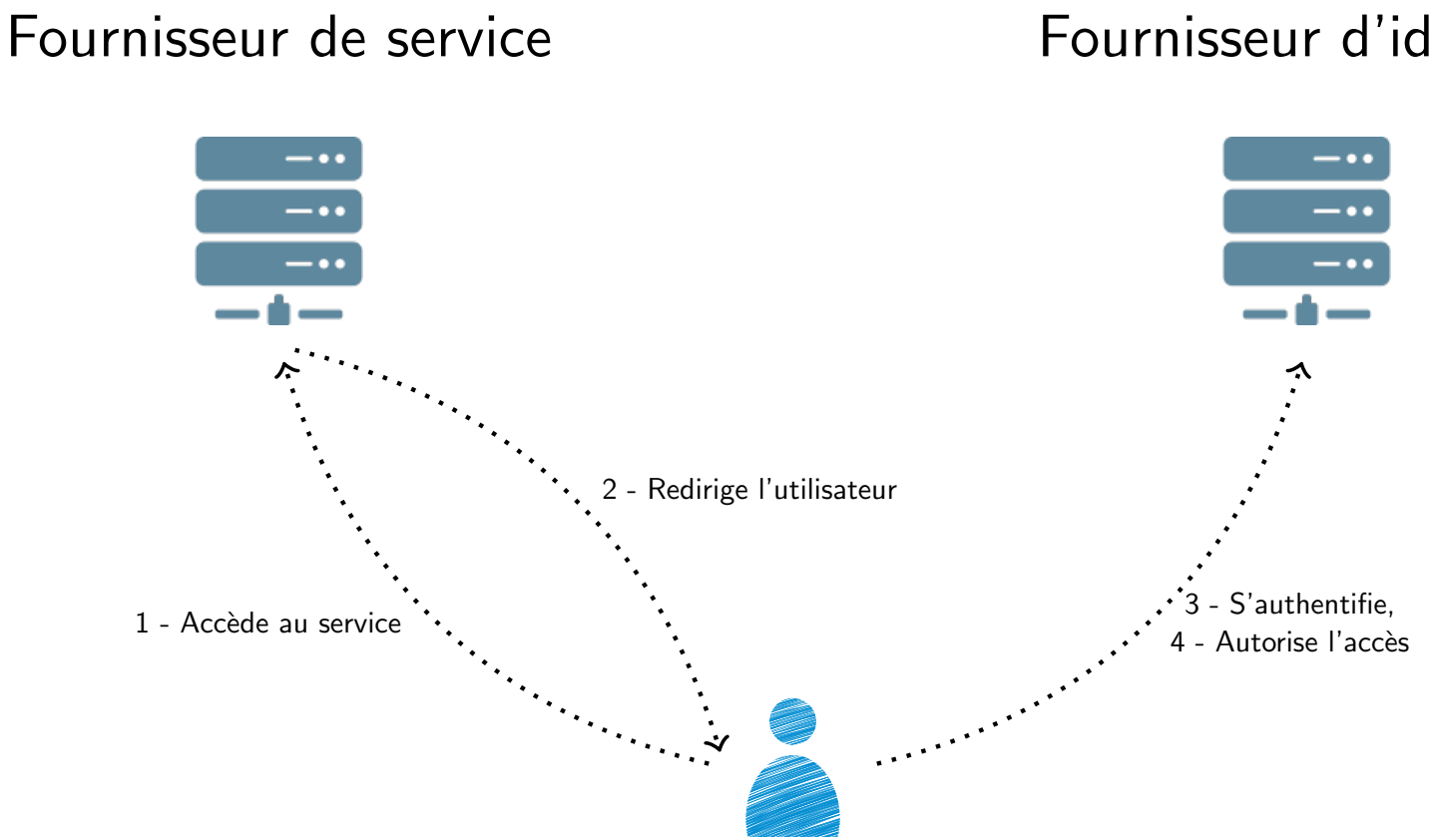
Architecture

Fournisseur de service

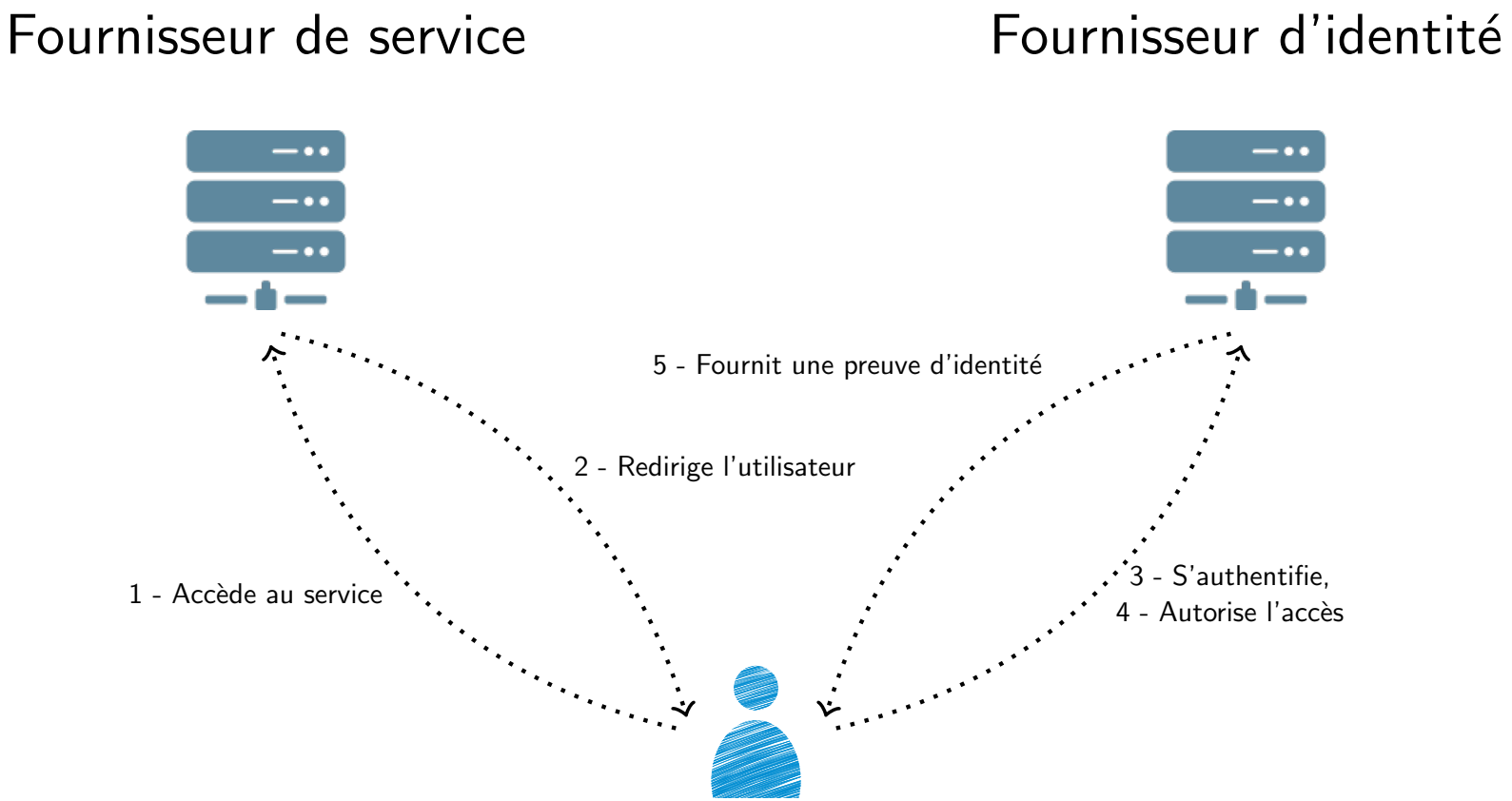
Fournisseur d'identité



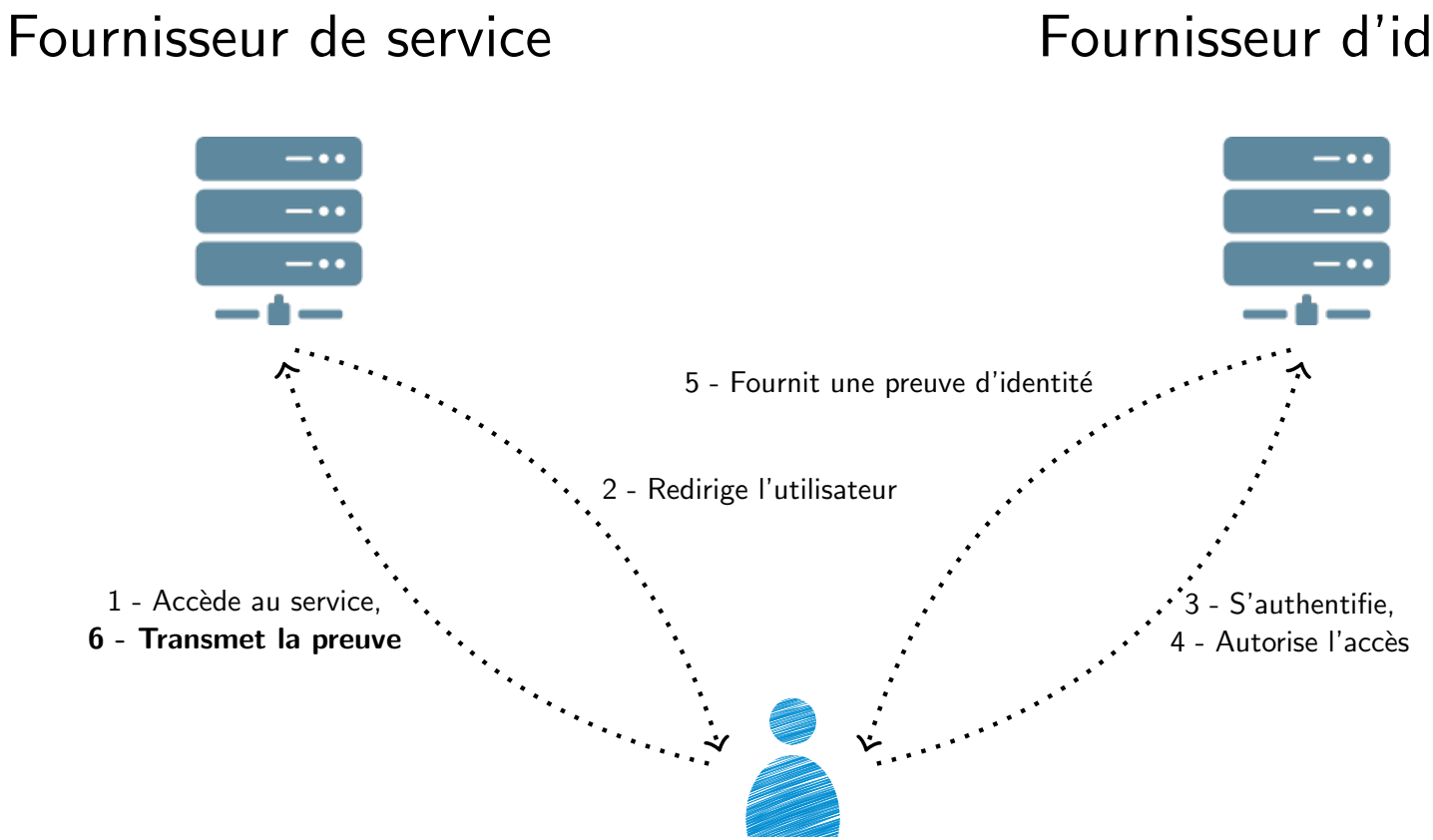
Architecture



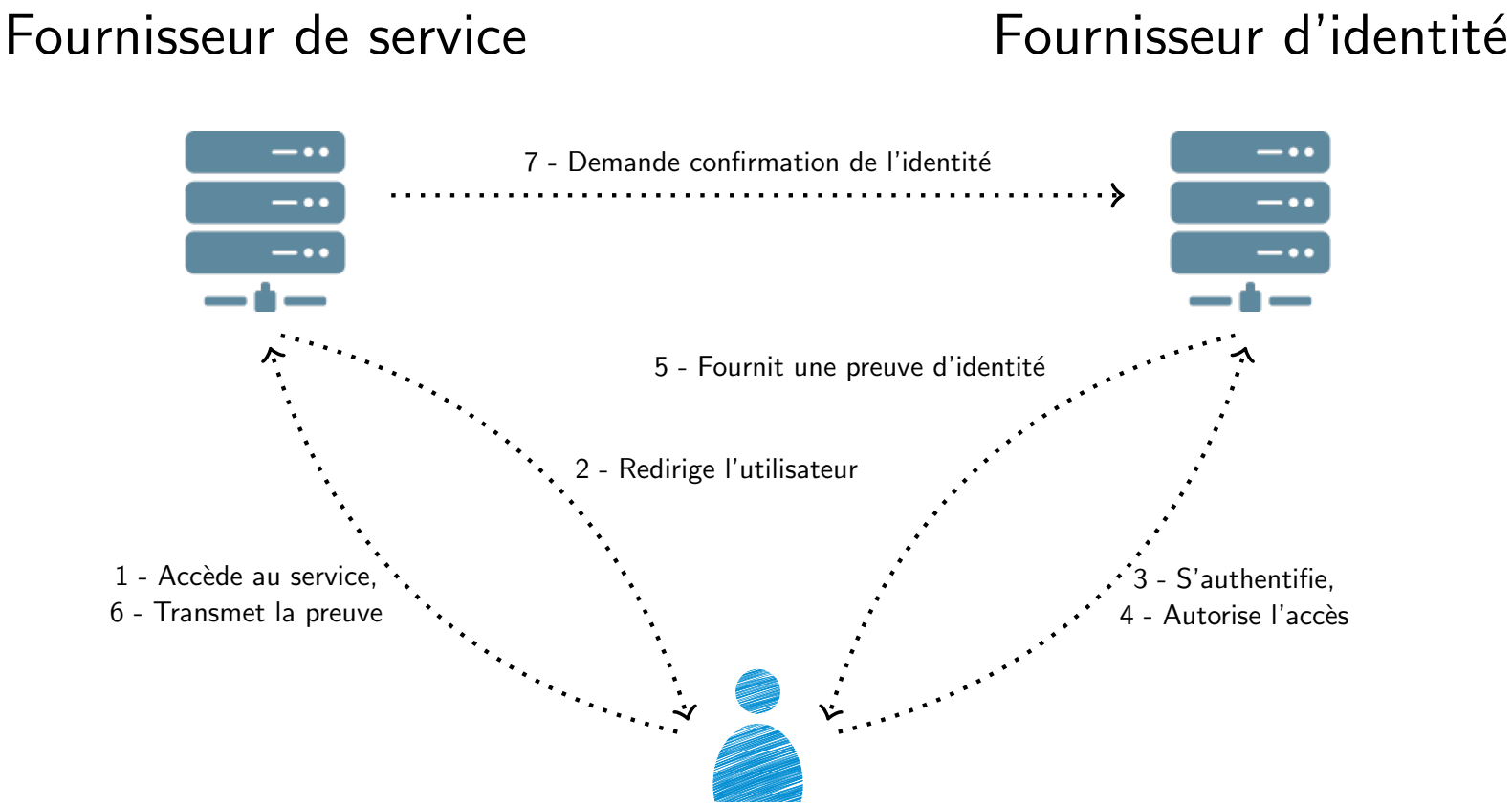
Architecture



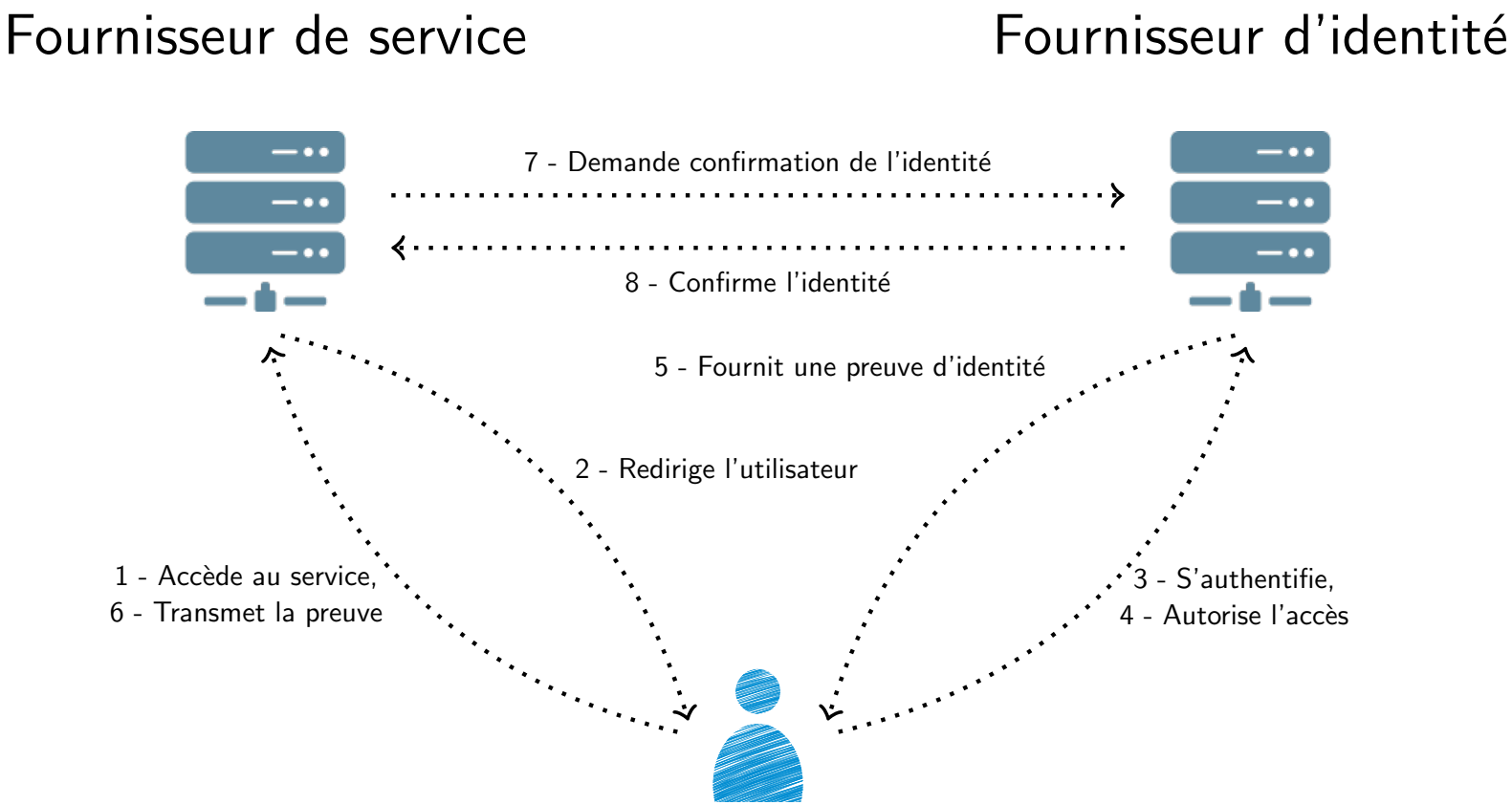
Architecture



Architecture



Architecture



OpenID

- Protocole d'*authentification*
- TODO

Protocole OAuth

- Protocole d'*autorisation*
- Actuellement en version 2.0
- Supporté par les géants du web
  - Google, Facebook, Slack...

- Ne parle plus d'*identités* mais de *ressources*
  - Propriétaire de ressources (Resource owner)
  - Serveur de ressources (Resource server)
  - Application cliente (Client)

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

- Récupérer les informations de son profil

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

- Récupérer les informations de son profil
- Ajouter un évènement dans son calendrier

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

- Récupérer les informations de son profil
- Ajouter un évènement dans son calendrier
- Envoyer des mails en son nom

Protocole OAuth - explications

- Permet d'autoriser une application tierce à accéder à une ressource

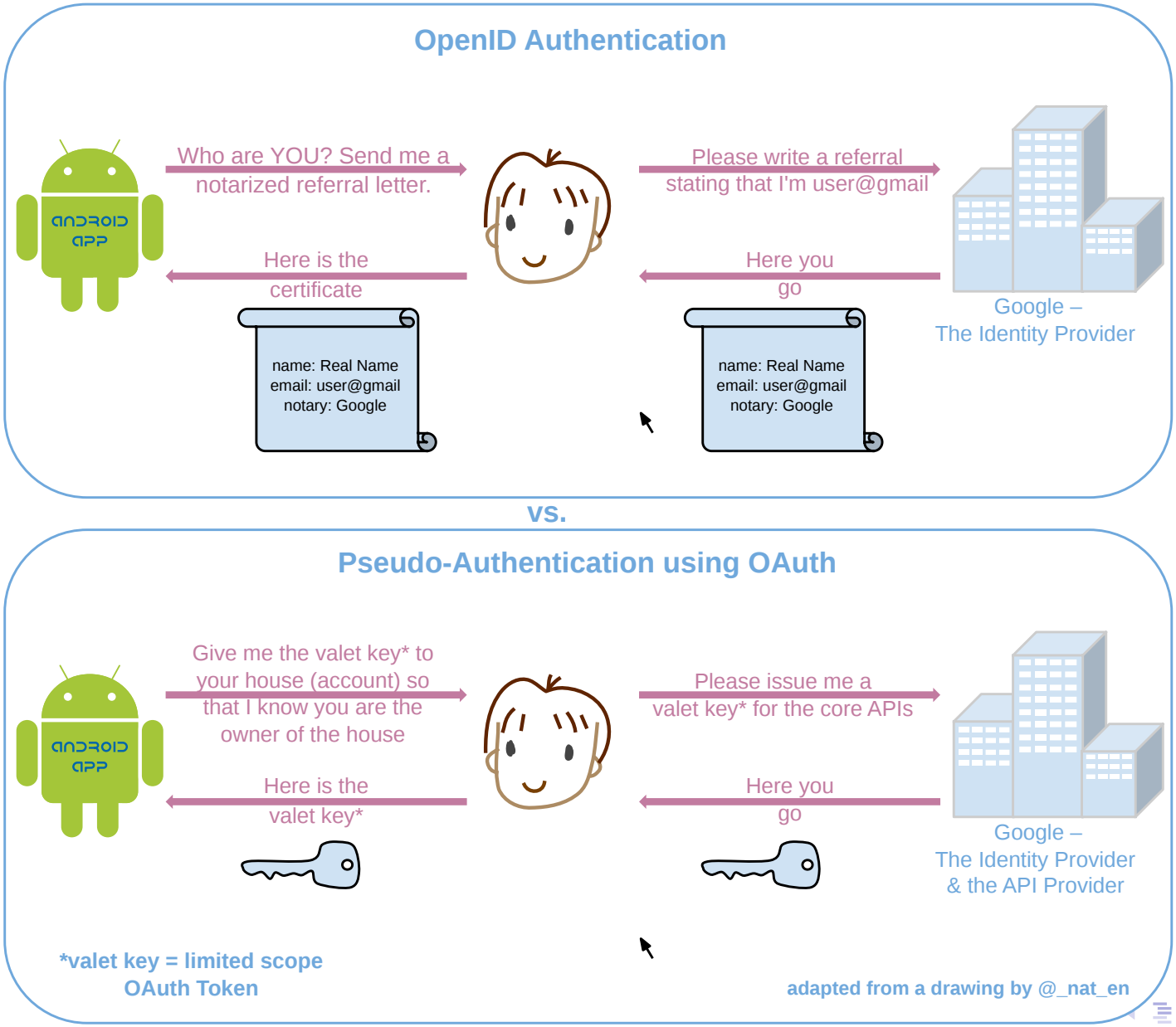
OAuth avec Google

Permet de donner l'autorisation à un service de:

- Récupérer les informations de son profil
- Ajouter un évènement dans son calendrier
- Envoyer des mails en son nom

- Utilisé de façon détournée pour faire de la *pseudo-authentification*

Différences entre OpenID & OAuth



OpenID Connect

- Nouveau protocole basé sur OAuth 2.0

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Scalabilité
  - Single Sign-On

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Scalabilité
  - Single Sign-On
- Inconvénients
  - Plus *complexe* à bien implémenter
  - Dépendant de services tiers
    - Disparition du fournisseur d'identité?
    - Fournisseur d'identité compromis?

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Scalabilité
  - Single Sign-On
- Inconvénients
  - Plus *complexe* à bien implémenter
  - Dépendant de services tiers
    - Disparition du fournisseur d'identité?
    - Fournisseur d'identité compromis?
- Mais rien n'empêche d'implémenter son propre fournisseur d'identité

Authentification déléguée

Frameworks & Librairies

- Available at `https://plm.telecomnancy.univ-lorraine.fr`

Questions

Merci pour votre attention, avez-vous des questions?