Mécanismes d'authentification

État de l'art

Matthieu Nicolas

20/09/2016

Plan

Plan

Authentification locale

Principe

- Architecture la plus *intuitive*
- L'application propose son propre système d'authentification

Authentification locale

Architecture

- TODO

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*
  - Complexe de répliquer l'environnement
  - Un compte supplémentaire pour l'utilisateur...

Authentification locale

Frameworks & Librairies

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

Plan

Authentification déléguée

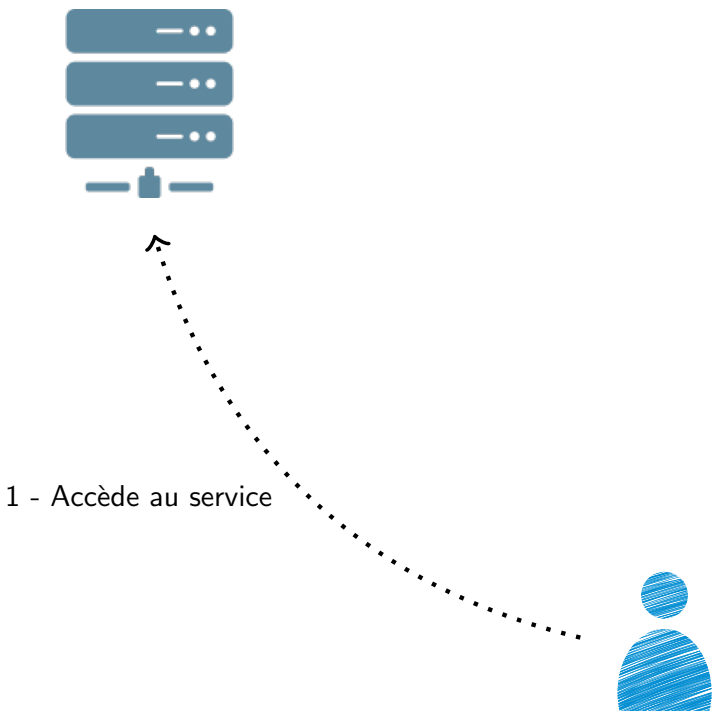
Principe

- 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

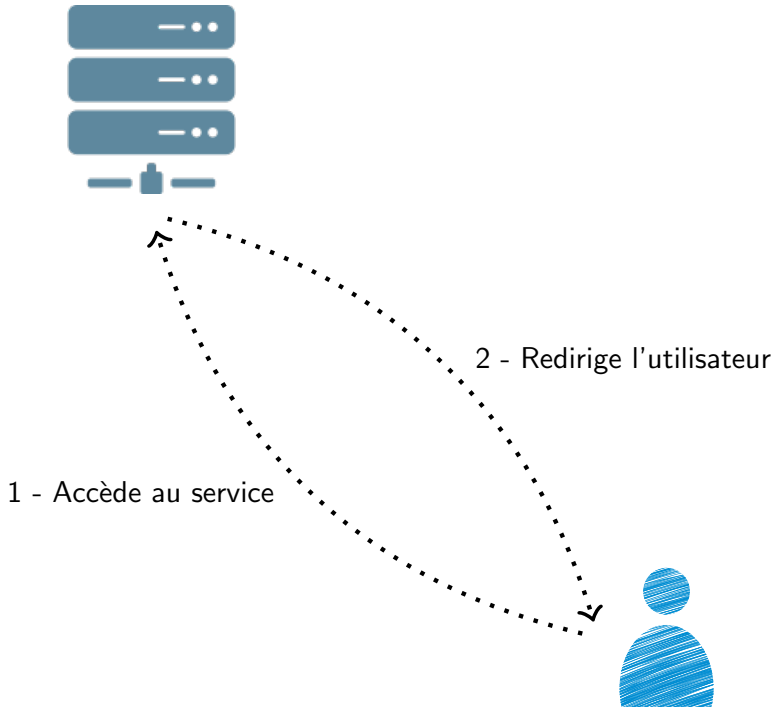
Fournisseur d'identité



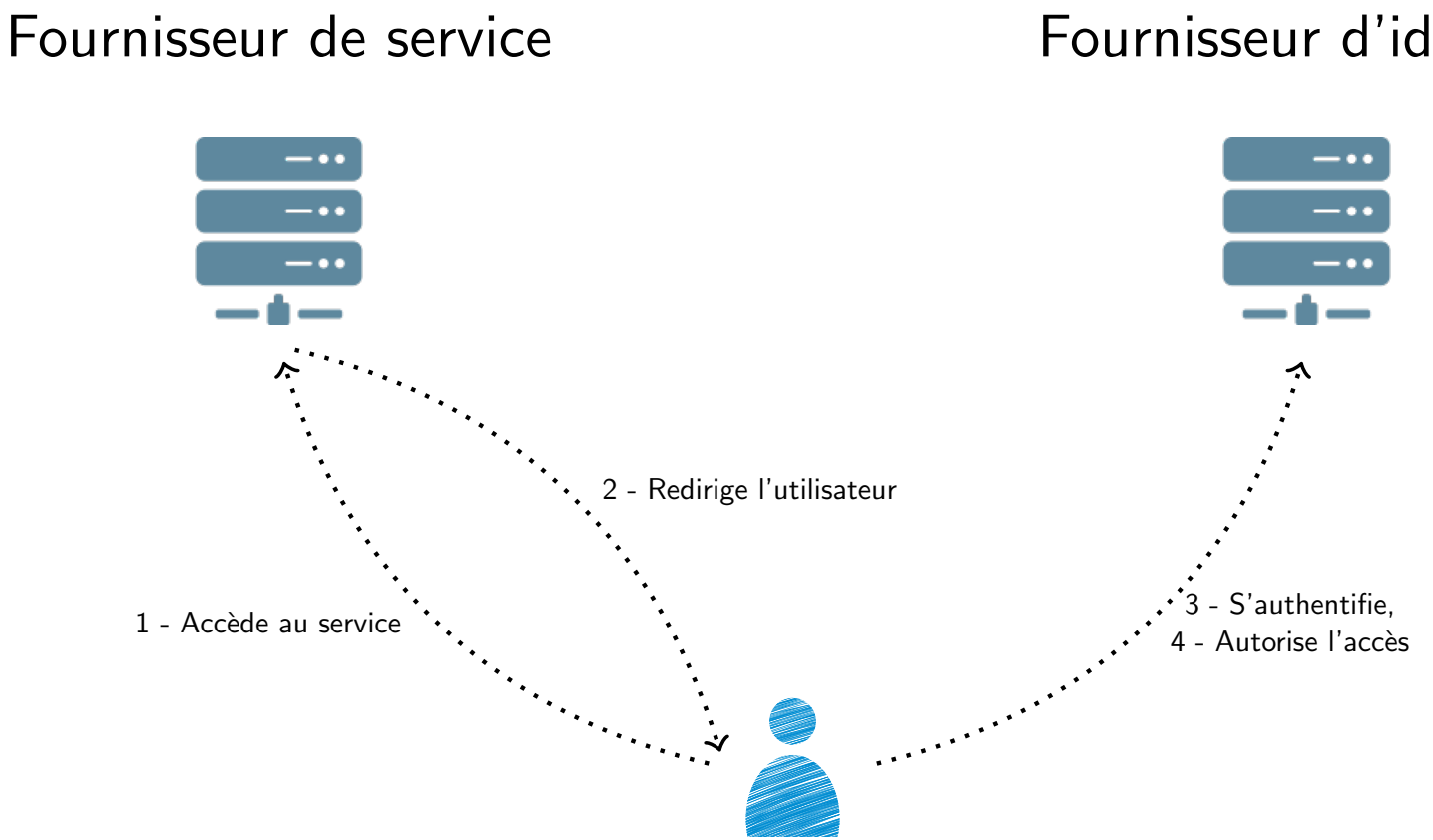
Architecture

Fournisseur de service

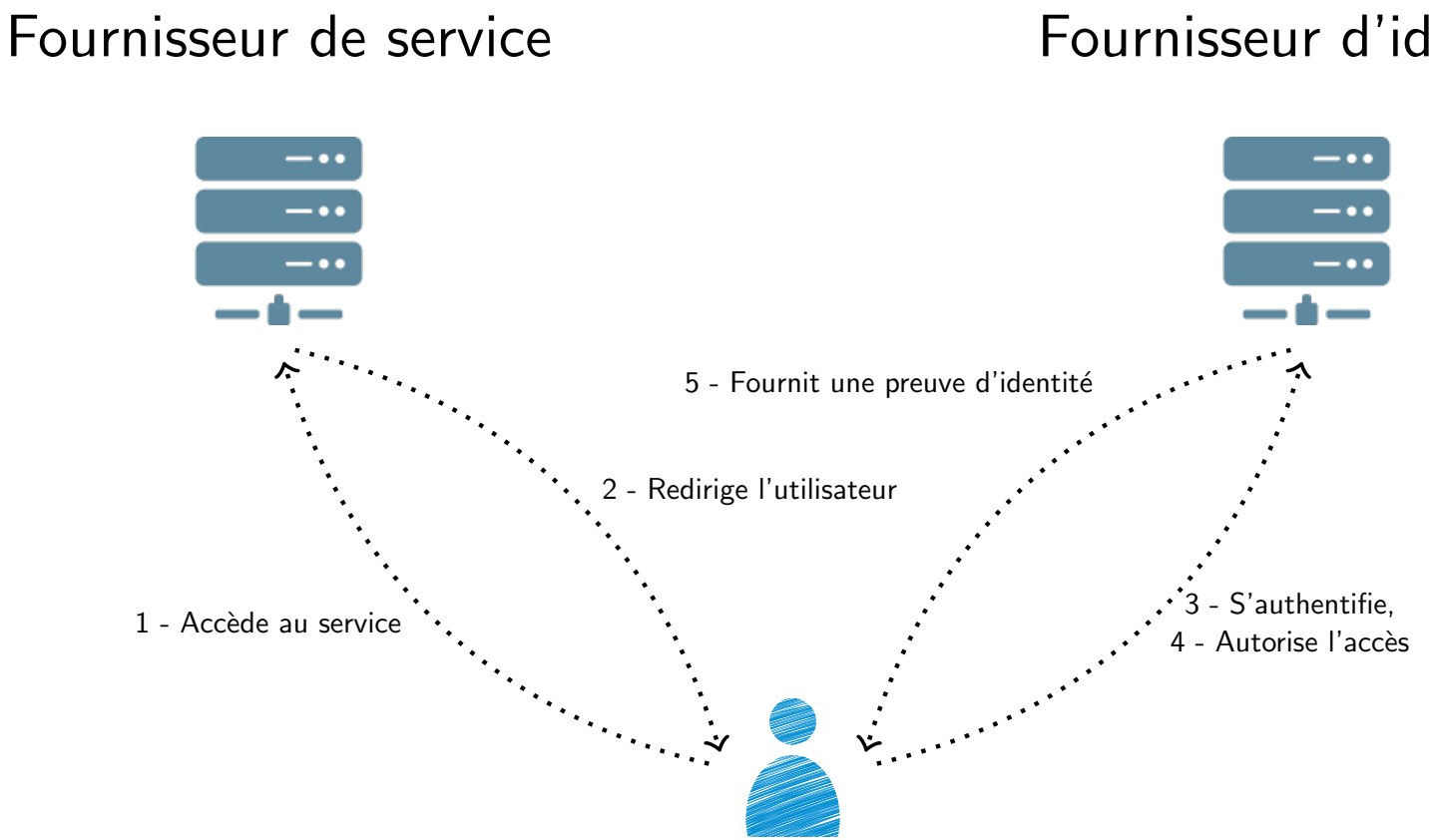
Fournisseur d'identité



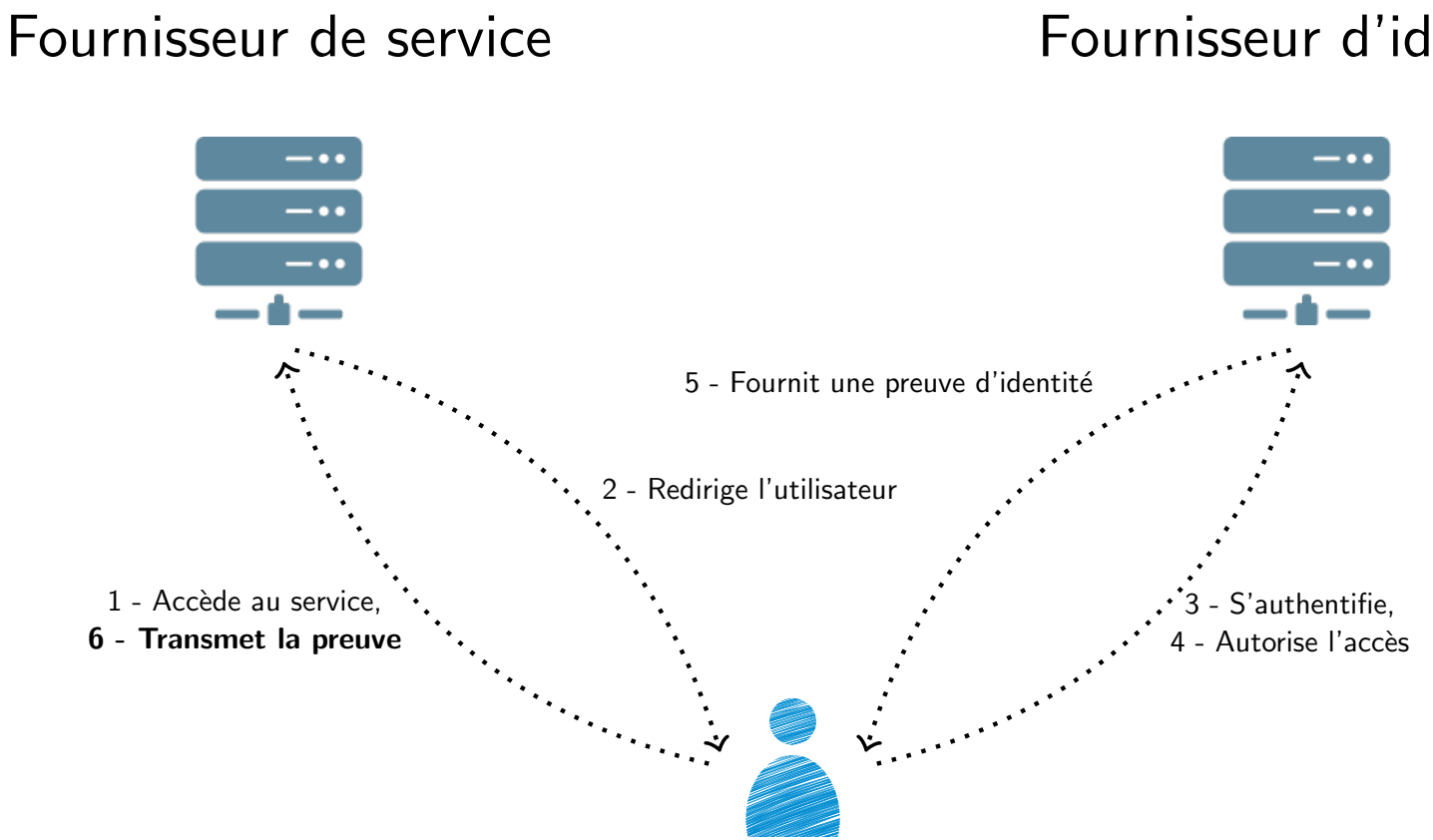
Architecture



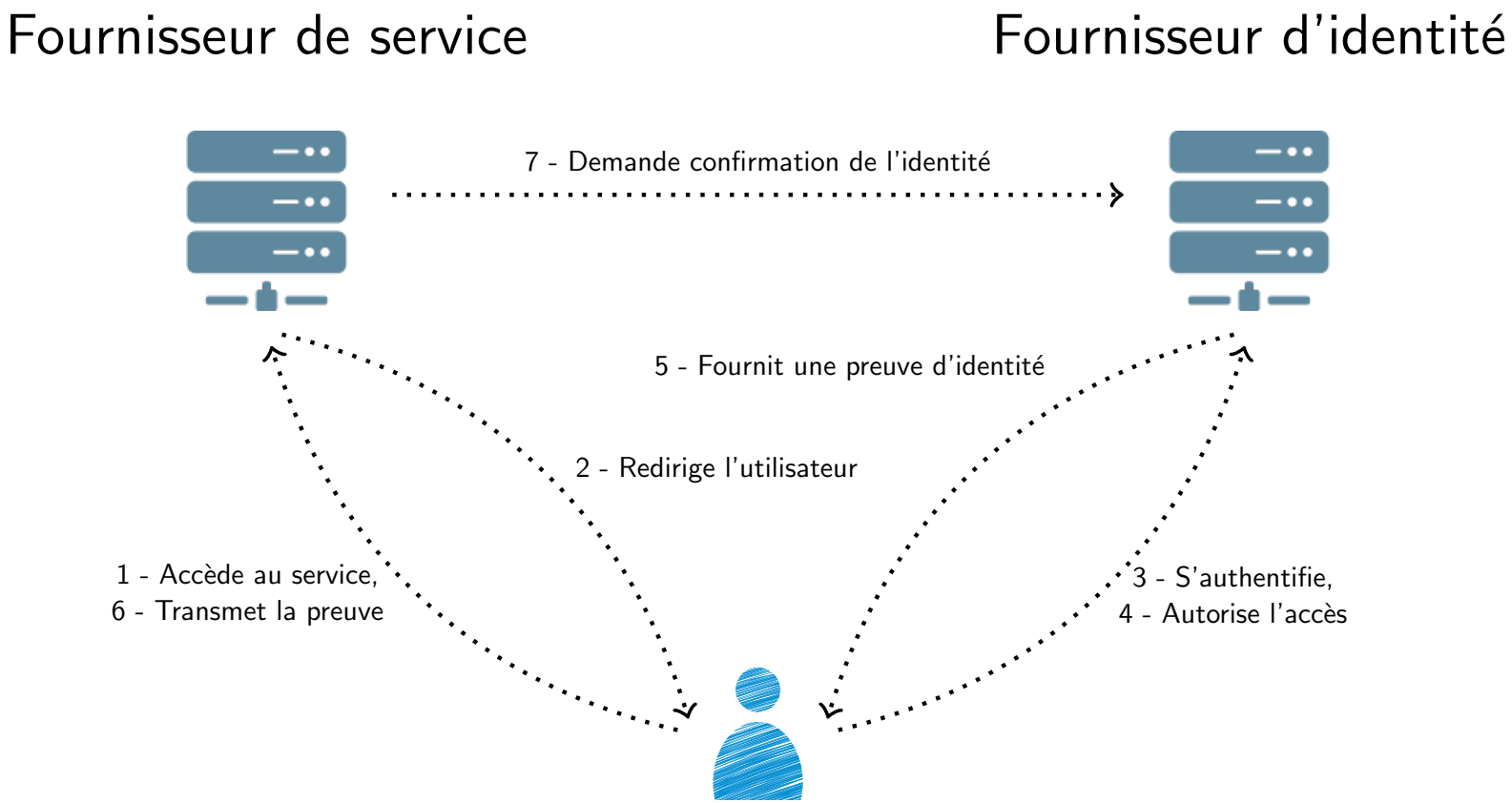
Architecture



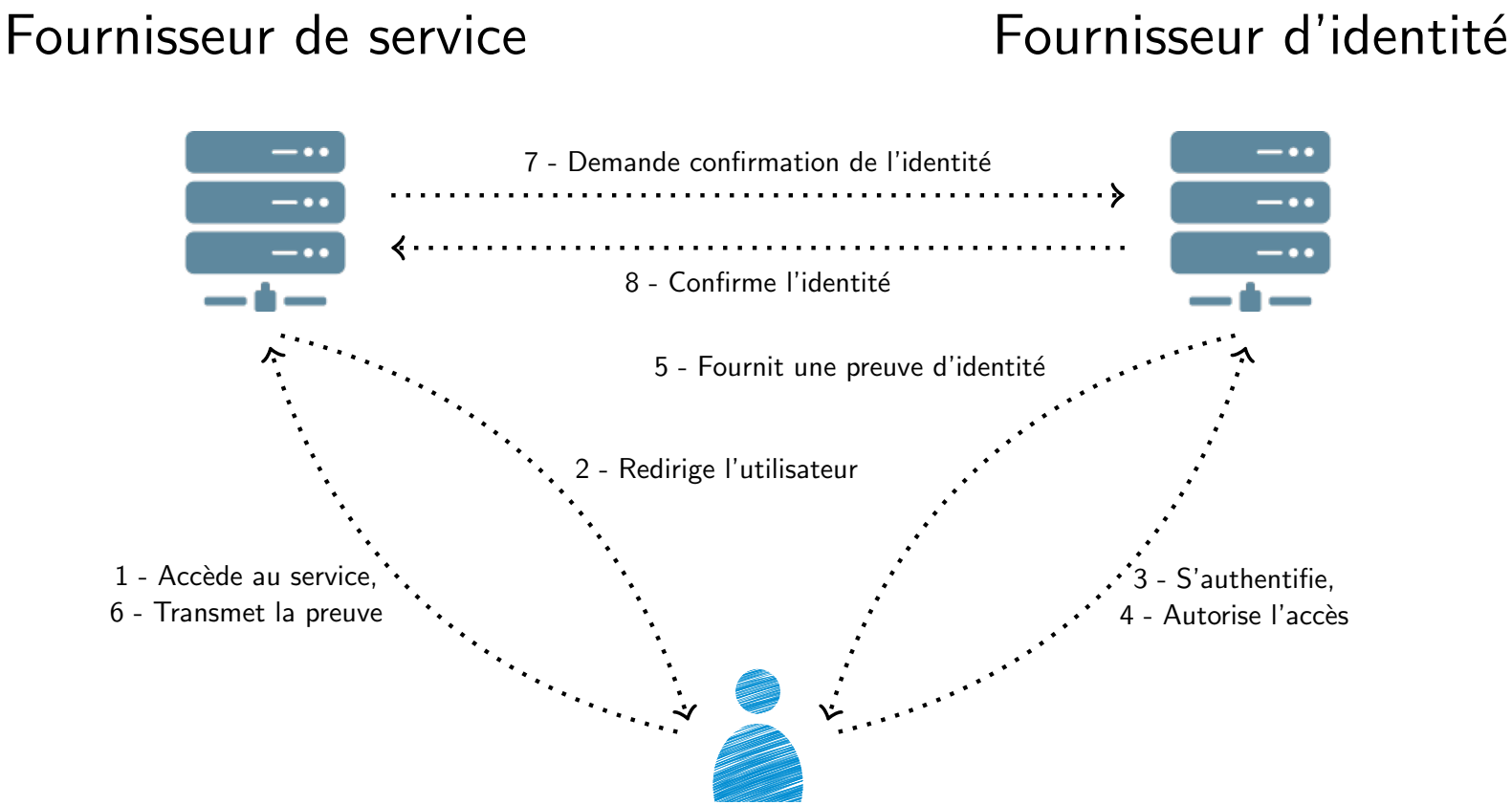
Architecture



Architecture



Architecture



OpenID

- Protocole d'*authentification*
- TODO

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la ressource

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la ressource

OAuth avec Google

Permet de donner l'autorisation à un service de:

- Récupérer les informations de son profil

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la 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

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la 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

OAuth

- Protocole d'*autorisation*

- Ne parle plus de fournisseur d'identité...
- ... Mais de **serveur de ressources (Resource server)**
- Permet au propriétaire d'une ressource (**Resource owner**) d'autoriser une application tierce à accéder à la ressource

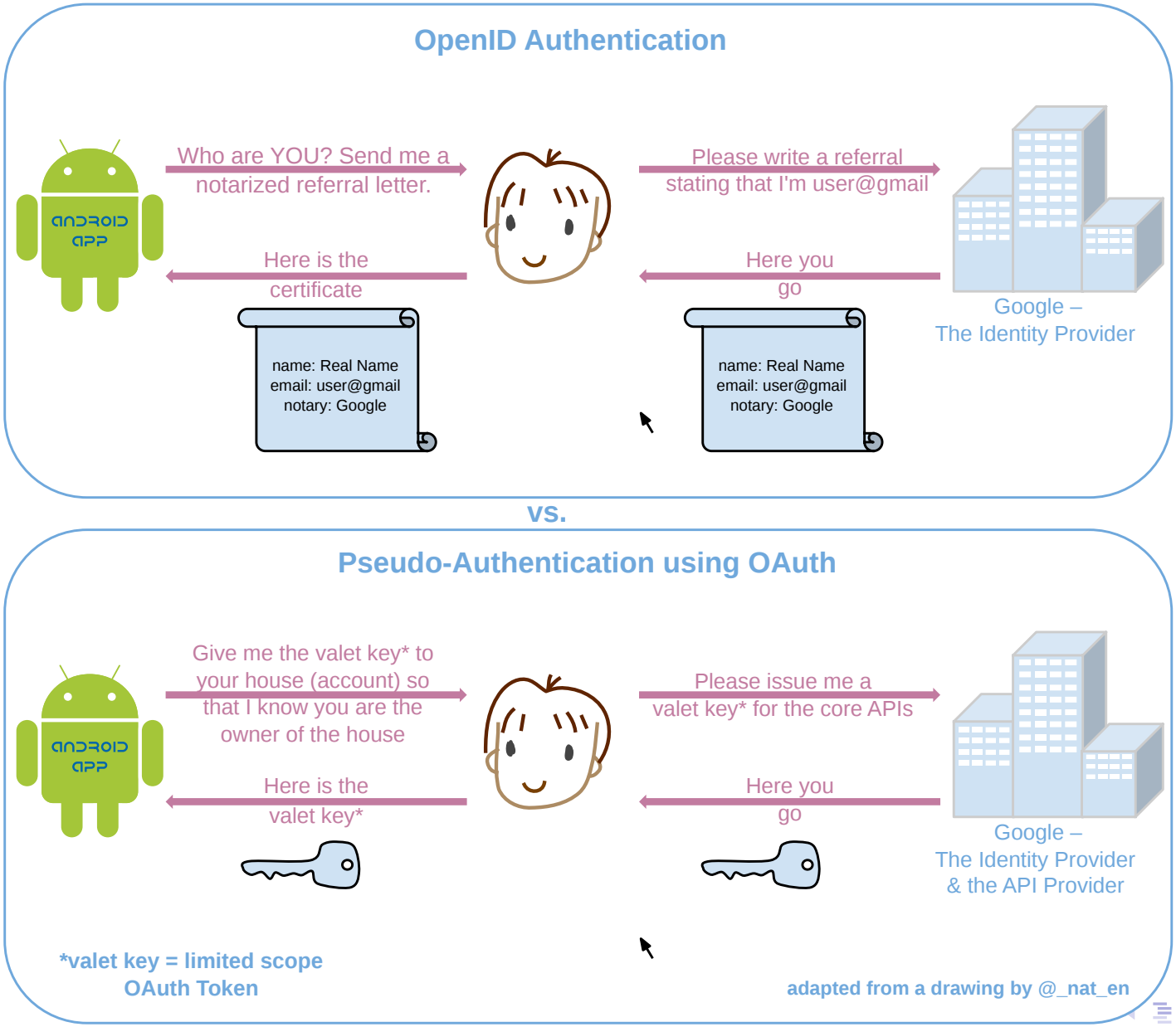
OAuth avec Google

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

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

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Flexibilité
  - Scalabilité
  - SSO
  - Pas besoin de partager les credentials

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Flexibilité
  - Scalabilité
  - SSO
  - Pas besoin de partager les credentials

- Inconvénients
  - Plus *complexe* à bien implémenter
  - Dépendant de services tiers
    - Disparation du fournisseur d'identité?
    - Fournisseur d'identité compromis?

Authentification déléguée

Avantages vs Inconvénients

- Avantages
  - Interopérabilité
  - Flexibilité
  - Scalabilité
  - SSO
  - Pas besoin de partager les credentials
- Inconvénients
  - Plus *complexe* à bien implémenter
  - Dépendant de services tiers
    - Disparation 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?