

La protection de la jeunesse en ligne

Authentification : application aux mineurs

Adrien Koutsos

Doctorant, LSV, ENS Paris-Saclay

26 janvier 2018

- 1 Introduction
- 2 L'authentification : qu'est-ce que c'est ?
- 3 Authentification par un tiers
- 4 Le projet IRMA

Introduction

Objectif

S'assurer de l'âge de l'utilisateur avant de donner l'accès à un site web.

Exemples d'applications

Pornographie, jeux d'argent (paris sportifs, poker ...).

Introduction

Objectif

S'assurer de l'âge de l'utilisateur avant de donner l'accès à un site web.

Exemples d'applications

Pornographie, jeux d'argent (paris sportifs, poker ...).

Difficulté

- Dans le monde "physique", la vérification de l'âge se fait à l'aide d'une pièce d'identité (CNI, permis de conduire, passeport) :
preuve de possession + vérification de l'authenticité du document.
- Comment réaliser cela sur internet ?

L'authentification : qu'est-ce que c'est ?

Définition : authentification en ligne

Processus permettant à un serveur (site web) de s'assurer de l'identité d'un utilisateur.

L'authentification : qu'est-ce que c'est ?

Définition : authentification en ligne

Processus permettant à un serveur (site web) de s'assurer de l'identité d'un utilisateur.

Exemple

- Banque en ligne :

identifiant + mot de passe

- Serveur e-mail :

adresse e-mail + mot de passe (+ téléphone portable)

Authentification en ligne

Méthode permettant l'authentification en ligne

- Preuve de connaissance (mot de passe).
- *Second facteur (facultatif) : preuve de possession (téléphone portable).*
- Nécessité d'une inscription préalable pour déterminer le secret commun (le mot de passe) entre le site web et l'utilisateur.

Authentification en ligne

Méthode permettant l'authentification en ligne

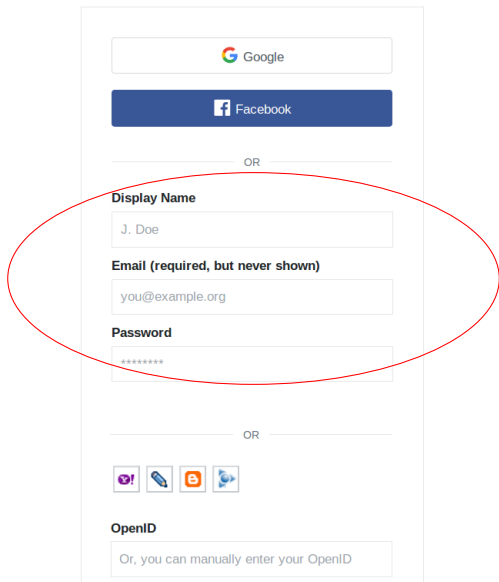
- Preuve de connaissance (mot de passe).
- *Second facteur (facultatif) : preuve de possession (téléphone portable).*
- Nécessité d'une inscription préalable pour déterminer le secret commun (le mot de passe) entre le site web et l'utilisateur.

Problèmes

- Une inscription par site web !
- Comment le site web s'assure de la véracité du nom/âge donné lors de l'inscription ?

- 1 Introduction
- 2 L'authentification : qu'est-ce que c'est ?
- 3 Authentification par un tiers**
- 4 Le projet IRMA

Un exemple : stackoverflow.com



The image shows a login and registration form. At the top, there are two buttons: a white one with the Google logo and a blue one with the Facebook logo. Below these is a horizontal line with the word "OR" in the center. The registration section is enclosed in a red oval and contains the following fields: "Display Name" with the value "J. Doe", "Email (required, but never shown)" with the value "you@example.org", and "Password" with a masked value of "*****". Below this section is another horizontal line with "OR" in the center. At the bottom, there are four small icons representing different OpenID providers: a purple one with an exclamation mark, a blue one with a pencil, an orange one with an 'S', and a blue one with a globe. Below these icons is the "OpenID" label and a text input field containing the text "Or, you can manually enter your OpenID".

1er possibilité :
inscription

Un exemple : stackoverflow.com

The image shows a login form with three main sections, each circled in red:

- Top Section:** Two buttons for third-party services: Google and Facebook.
- Middle Section:** A registration form with fields for:
 - Display Name:** J. Doe
 - Email (required, but never shown):** you@example.org
 - Password:** masked with asterisks (*****)
- Bottom Section:** A row of social media icons (Twitter, GitHub, etc.) and an **OpenID** field with the text "Or, you can manually enter your OpenID".

2nd possibilité :
services tiers

1er possibilité :
inscription

2nd possibilité :
services tiers

Authentification par un service tiers

Le protocole OpenID Connect

- Fournisseurs d'identité : Google, Facebook,...
- L'utilisateur s'inscrit une fois, et utilise la même identité sur plusieurs sites.

Authentification par un service tiers

Le protocole OpenID Connect

- Fournisseurs d'identité : Google, Facebook,...
- L'utilisateur s'inscrit une fois, et utilise la même identité sur plusieurs sites.

Application à l'authentification des mineurs

OpenID Connect ne garantit pas l'exactitude des informations données.

⇒ Il faut un organisme certificateur (p.ex. auth.gouv.fr).

Authentification par un service tiers

Serveur d'authentification
(*auth.gouv.fr*)

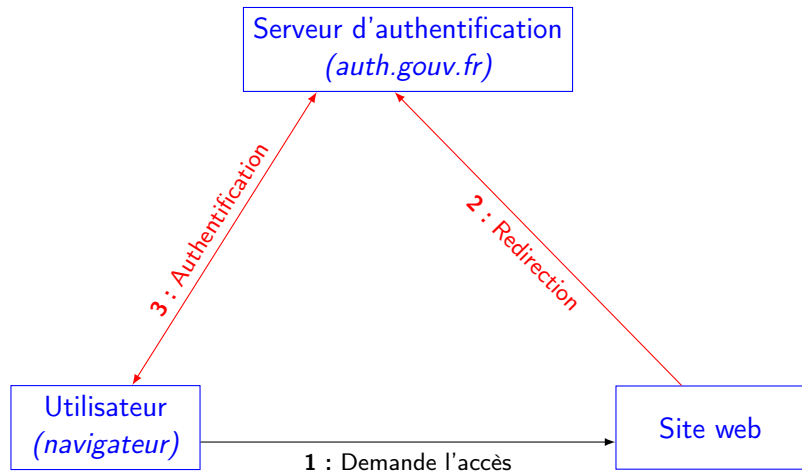
Utilisateur
(*navigateur*)

Site web

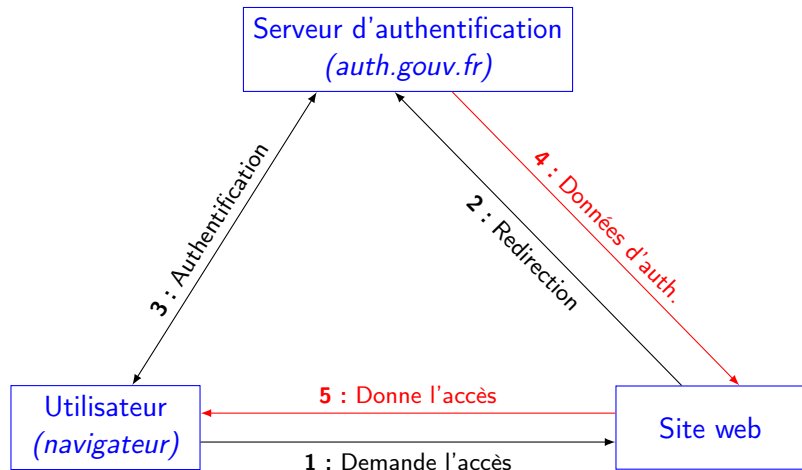
1 : Demande l'accès

```
graph LR; U["Utilisateur (navigateur)"] -- "1 : Demande l'accès" --> S["Site web"];
```

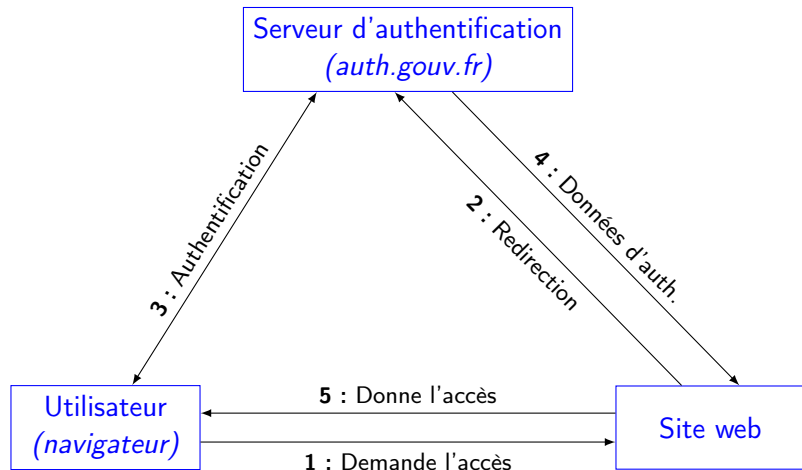
Authentification par un service tiers



Authentification par un service tiers



Authentification par un service tiers



Respect de la vie privée

Problèmes

- Le site web connaît le nom de l'utilisateur.
- Le serveur d'authentification (ex. le gouvernement) a accès au nom de tous les sites web visités.

Problèmes de respect de la vie privée.

Respect de la vie privée

Problèmes

- Le site web connaît le nom de l'utilisateur.
- Le serveur d'authentification (ex. le gouvernement) a accès au nom de tous les sites web visités.

Problèmes de respect de la vie privée.

Solutions

- Le site web n'a pas besoin de connaître l'identité de l'utilisateur, seulement de s'assurer qu'il n'est pas mineur.
Vérification d'un attribut de l'utilisateur.
- Le serveur d'authentification n'a pas besoin de connaître l'adresse du site web.

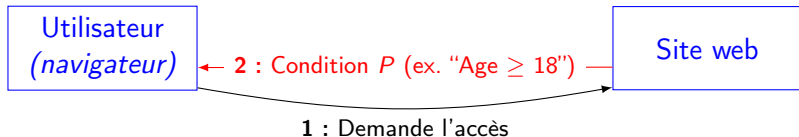
Authentification par un service tiers : version 2

Serveur d'authentification
(*auth.gouv.fr ?*)

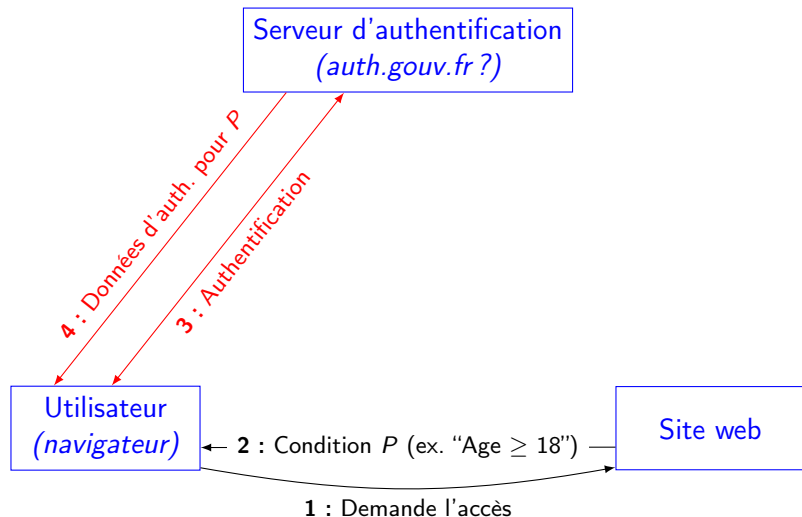


Authentification par un service tiers : version 2

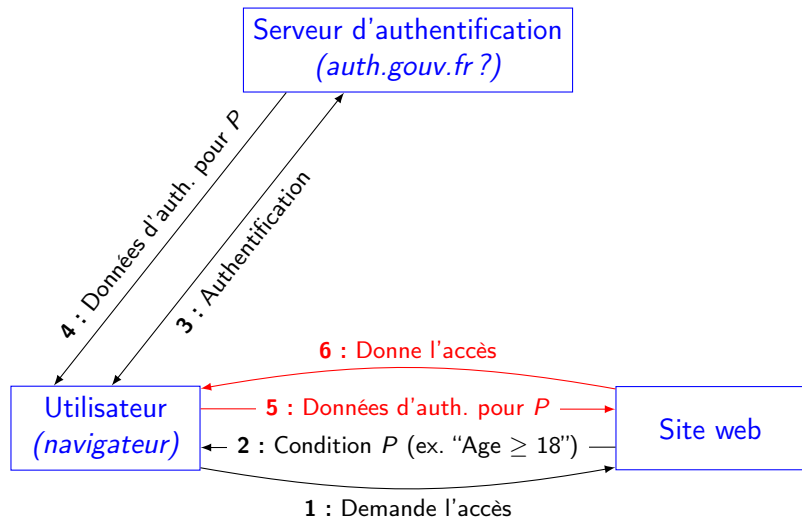
Serveur d'authentification
(*auth.gouv.fr ?*)



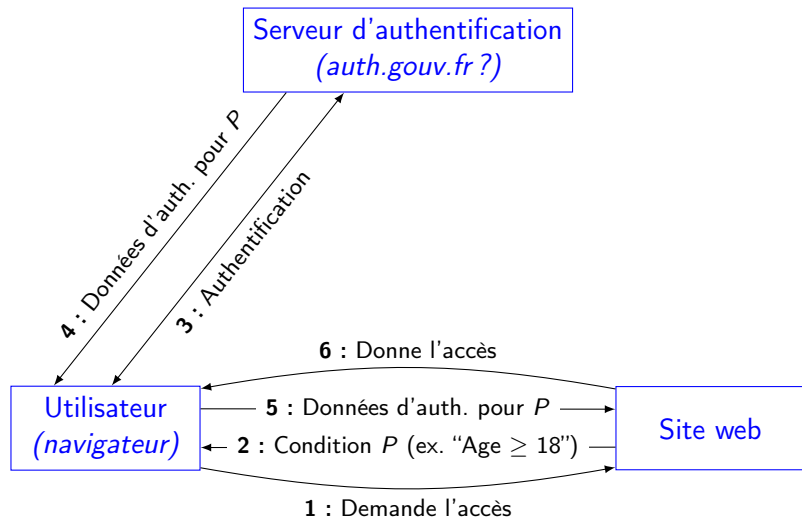
Authentification par un service tiers : version 2



Authentification par un service tiers : version 2



Authentification par un service tiers : version 2



- 1 Introduction
- 2 L'authentification : qu'est-ce que c'est ?
- 3 Authentification par un tiers
- 4 Le projet IRMA

Le projet IRMA

IRMA - I Reveal My Attributes

- Projet commencé à l'université de Radboud aux Pays-Bas.
- Va encore plus loin : **le serveur ne connaît pas vos attributs**. Il peut seulement certifier que ceux-ci sont authentiques.
(Technique cryptographique utilisée : Attribute Based Signatures, Zero-Knowledge Proofs)

Le projet IRMA

IRMA - I Reveal My Attributes

- Projet commencé à l'université de Radboud aux Pays-Bas.
- Va encore plus loin : **le serveur ne connaît pas vos attributs**. Il peut seulement certifier que ceux-ci sont authentiques.
(Technique cryptographique utilisée : Attribute Based Signatures, Zero-Knowledge Proofs)

Fonctionnement

- 1 Installer l'application et créer un compte.
- 2 Ajouter des attributs certifiés : université (SURFconext), banque (iDIN), ...
- 3 S'authentifier sur des sites web à travers l'application.

Le projet IRMA

Attributs certifiés disponibles

- Nom/Prénom
- Adresse
- E-mail
- Âge
- Numéro de téléphone
- Étudiant

Le projet IRMA

Attributs certifiés disponibles

- Nom/Prénom
- Adresse
- E-mail
- Âge
- Numéro de téléphone
- Étudiant

Propriétés

- Authenticité des attributs.
Exemple : l'utilisateur ne peut pas mentir sur son âge.
- Pas d'usurpation d'identité.
- Respect de la vie privé :
 - ▶ l'utilisateur choisit les attributs qu'il révèle.
 - ▶ le serveur d'authentification ne connaît pas les sites web visités.
- ...

Conclusion

Authentification : application aux mineurs

- L'authentification des mineurs est possible.
- Nécessité d'un organisme certificateur.
- Des projets similaires existent (p.ex. IRMA).

Difficultés

- Attention aux problèmes de respect de la vie privée.
- Il faut que les sites web appliquent la règle.

Merci pour votre attention.