

Beyond password: Time for a change



Olivier Potonniée
Octobre 2013

How can web applications authenticate their online users?

Often...

Create Your Account

* Required Information

Account Information

* Username	<input type="text"/>
* Password	<input type="password"/>
* Confirm Password	<input type="password"/>
* Email	<input type="text"/>

Please send me email updates!

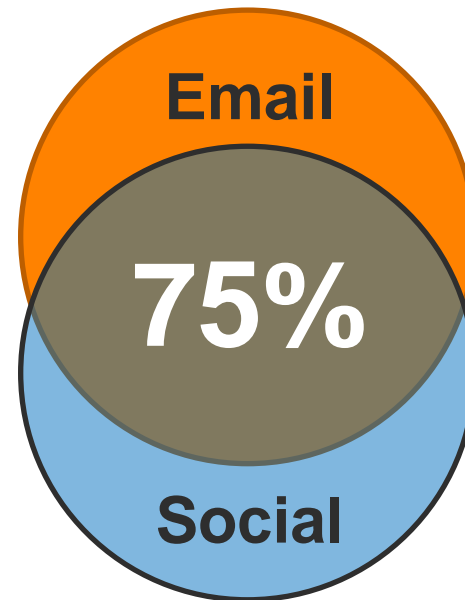
By creating my account I have read and agree to the [Terms of Service](#) and [Privacy Policy](#)

Create Account

Attacks

✦ Compromised passwords in 2013:

- ✦ Living Social: 50 millions
- ✦ EverNote: 50 millions
- ✦ Drupal: 1 million
- ✦ Twitter: 250,000
- ✦ ...



([BitDefender](#))

Strong Authentication

- ✦ At least 2 of:
 - ✦ Something you know (password, pin, etc.)
 - ✦ Something you have (card, mobile, etc.)
 - ✦ Something you are (biometrics)
- ✦ Independents, protected

Authenticate with OTP device

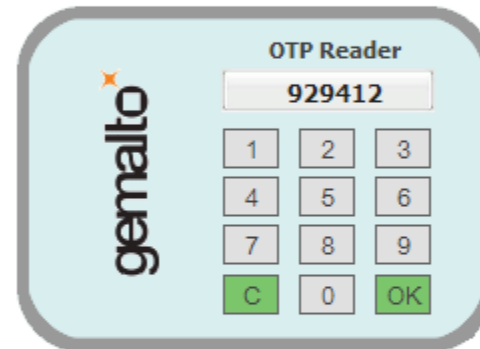
Protiva
Cloud Confirm

The inserted secure document can be used for OTP authentication. Please use the PinPad reader to generate an OTP; then enter Username, Password, and this OTP to login.

Username:

Password:


OTP:



Copyright © 2011 Gemalto. All rights reserved.



Authenticate with e-ID card



Please enter your PIN

BioPIN		
PIN		
4	6	3
7	9	0
1	2	8
C	5	OK

Copyright © 2011 Gemalto. All rights reserved.



Authenticate with e-ID card



Scan your right index

BioPIN



PIN

Copyright © 2011 Gemalto. All rights reserved.



Authenticate with Mobile ID



Please enter your mobile username and optionally select a mobile phone, then follow the instructions shown below.

Mobile Username: Select mobile phone

Phone Nickname:

Login

Cancel

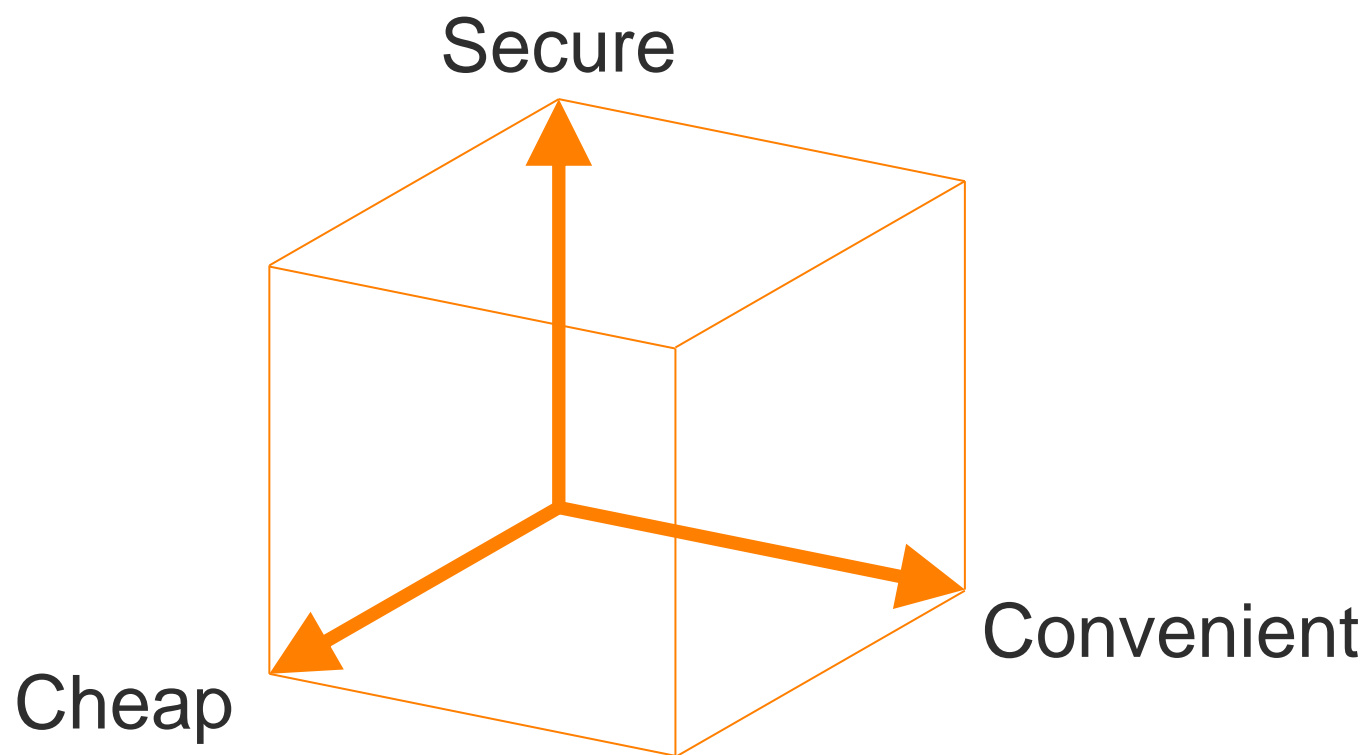
Authentication Code:

After pressing Login, please check your mobile phone for the authentication code that will appear in blue text in the space above. Press OK on your phone to sign.

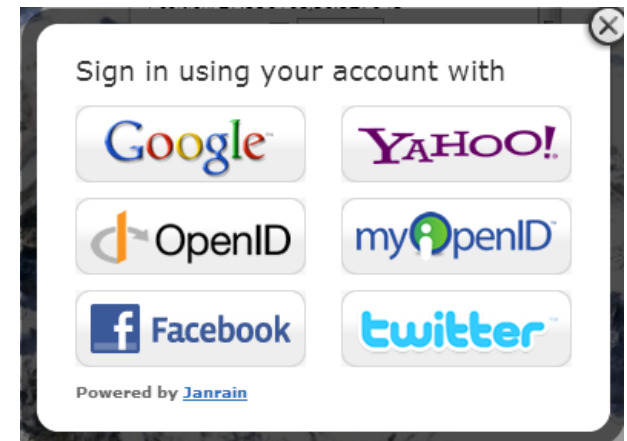
Copyright © 2011 Gemalto. All rights reserved.



Need to define YOUR solution

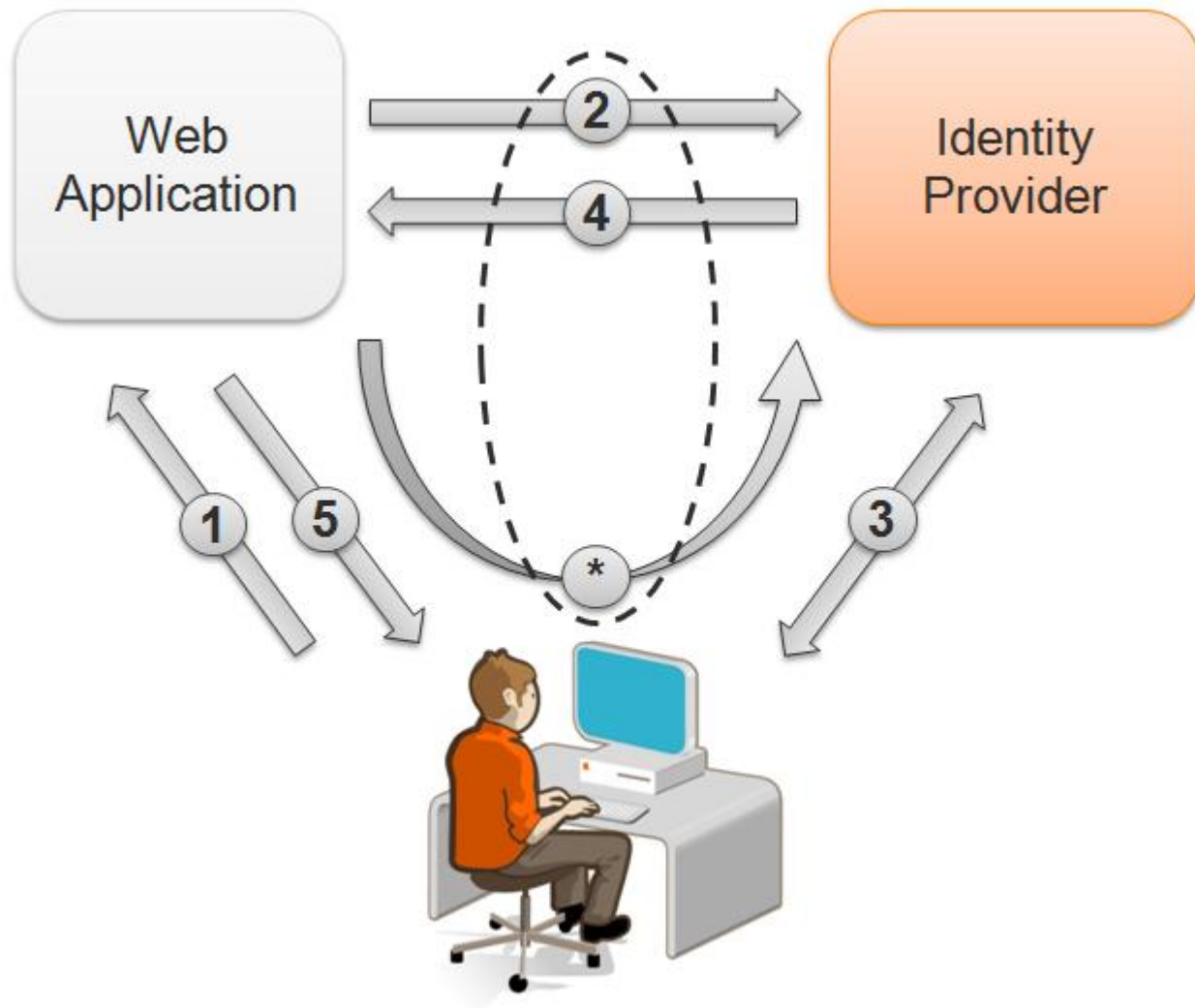


Social Login



- ✧ Identity reuse
 - ✧ Simpler for users (no new identifier to remember)
 - ✧ Single-Sign-On (SSO)
- ✧ Alleviate the application
- ✧ Privacy risks
 - ✧ Traceability
 - ⚠ Disclosure of personal data

Authentication delegation



Delegation protocols



Browser ID

OASIS SAML



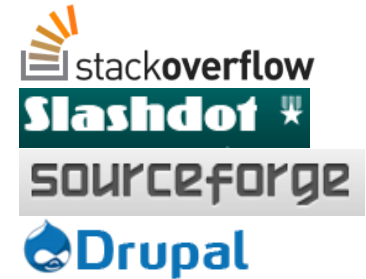
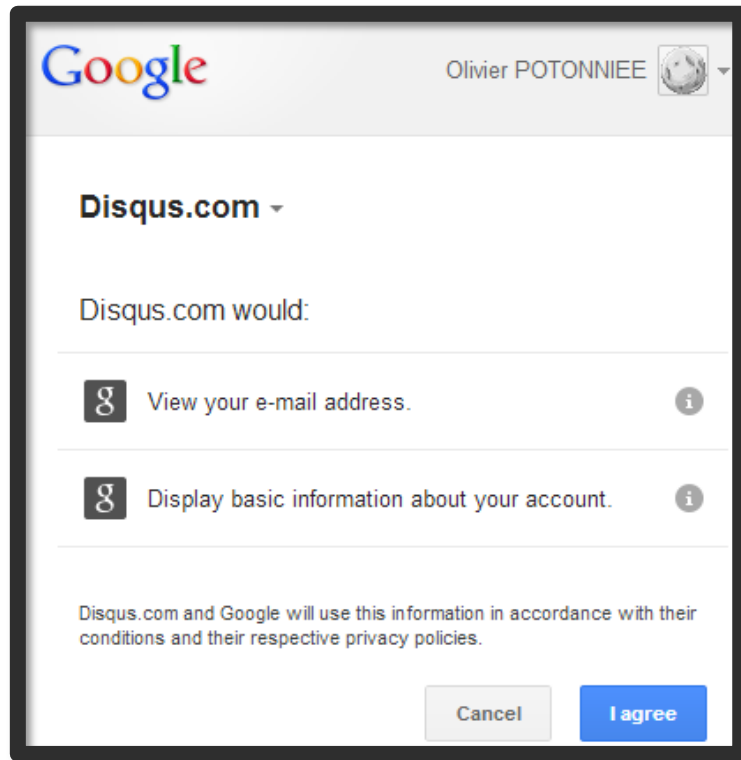
OAuth



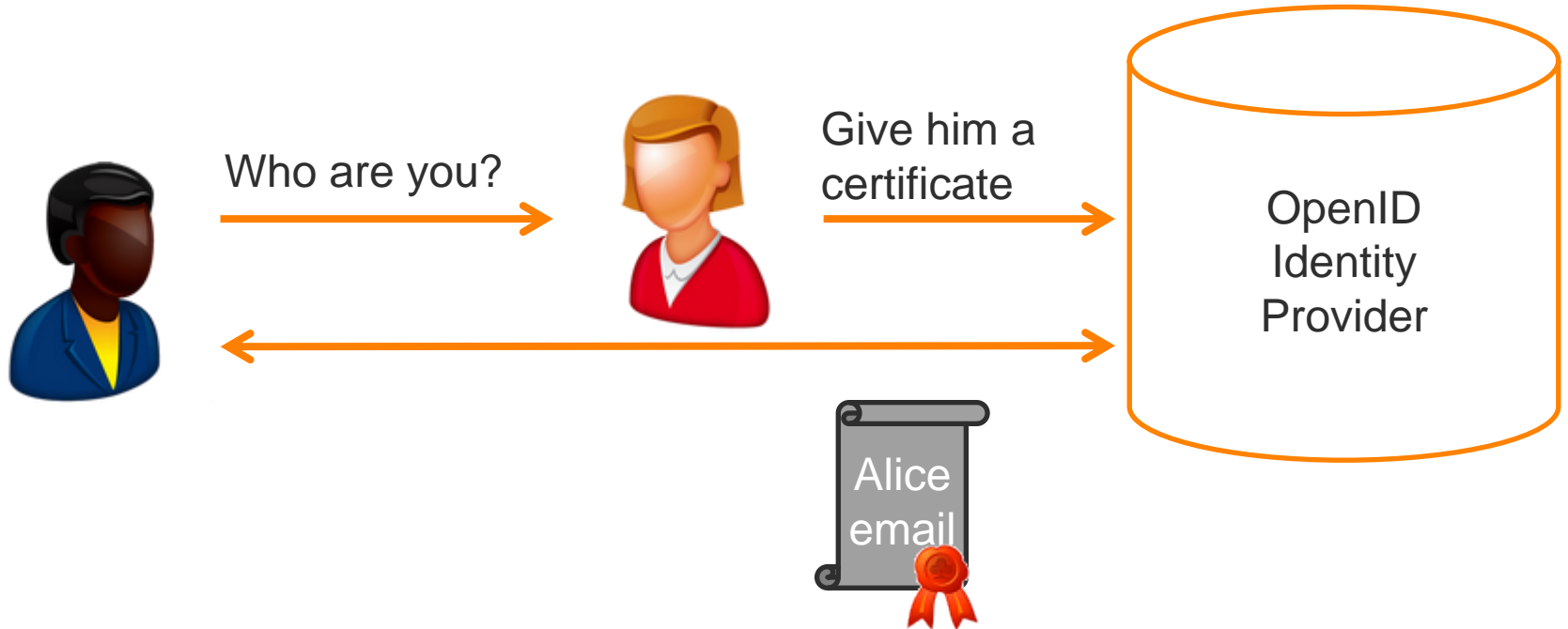


A simple URL

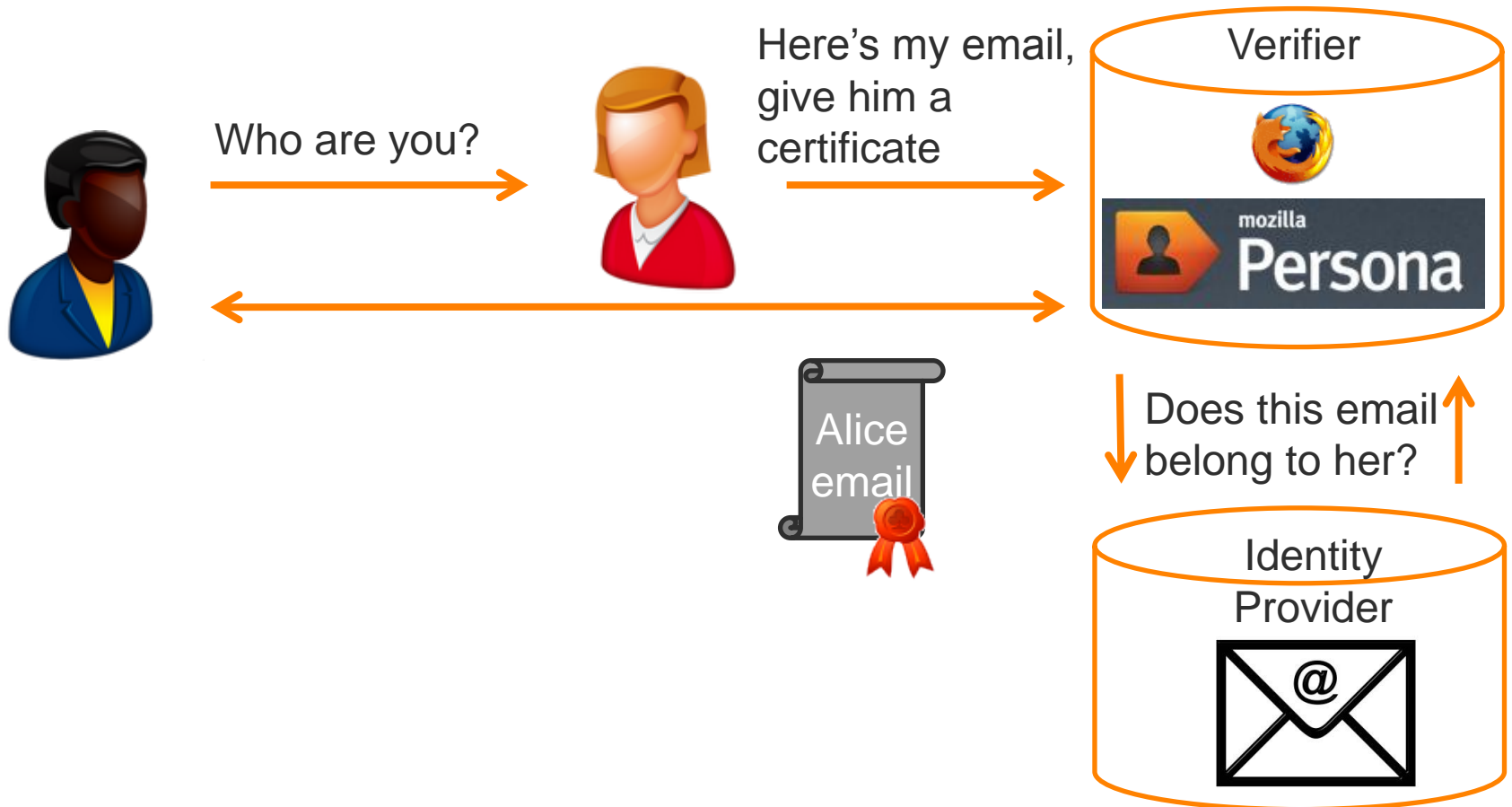
Your OpenID:



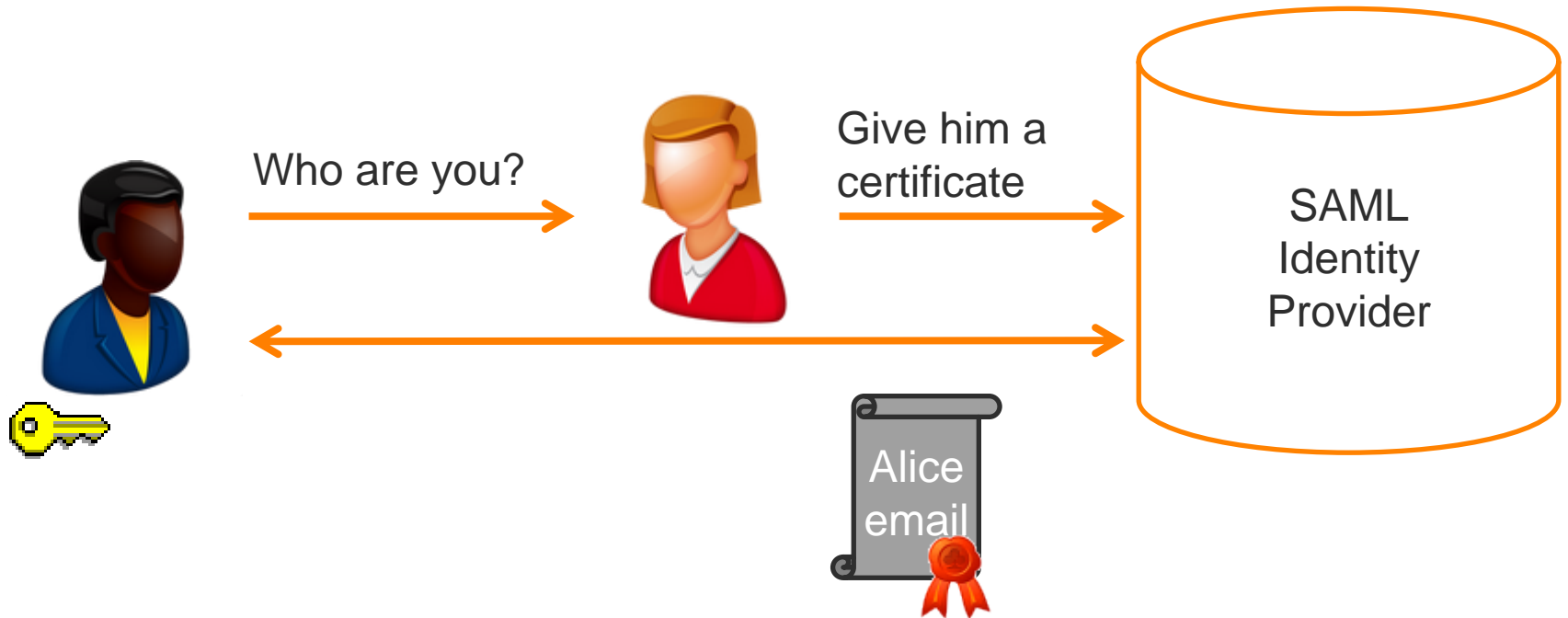
OpenID Authentication



([nat sakimura](#))



OASIS SAML Assertions





OAuth Authorization to access personal data

Login with Facebook

DISQUS receive the following information: your public profile, **friends list** and email address.

Terms of application · Privacy Policy

Cancel

Authorize LiveJournal.com to use your account?

This application **will be able to**:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

Authorize app Cancel

This application **will not be able to**:

- Access your direct messages.
- See your Twitter password.

Google Olivier POTONNIEE

USA TODAY USA TODAY

App request your permission to:

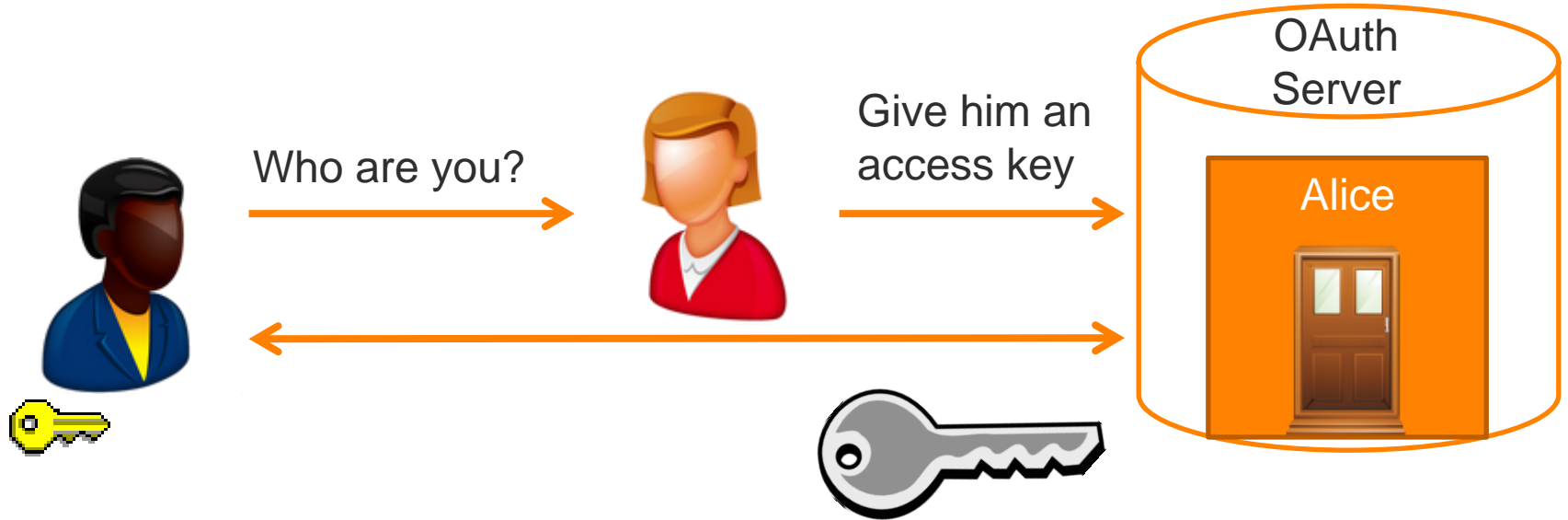
- See the basic information of your profile and the list of people from your circles. (Edit List)
- Allow Google to inform members of the circles that you are connected to this application with Google:
 - Vos cercles
 - + Ajouter des contacts
- You only
- View your e-mail address.
- Display basic information about your account.

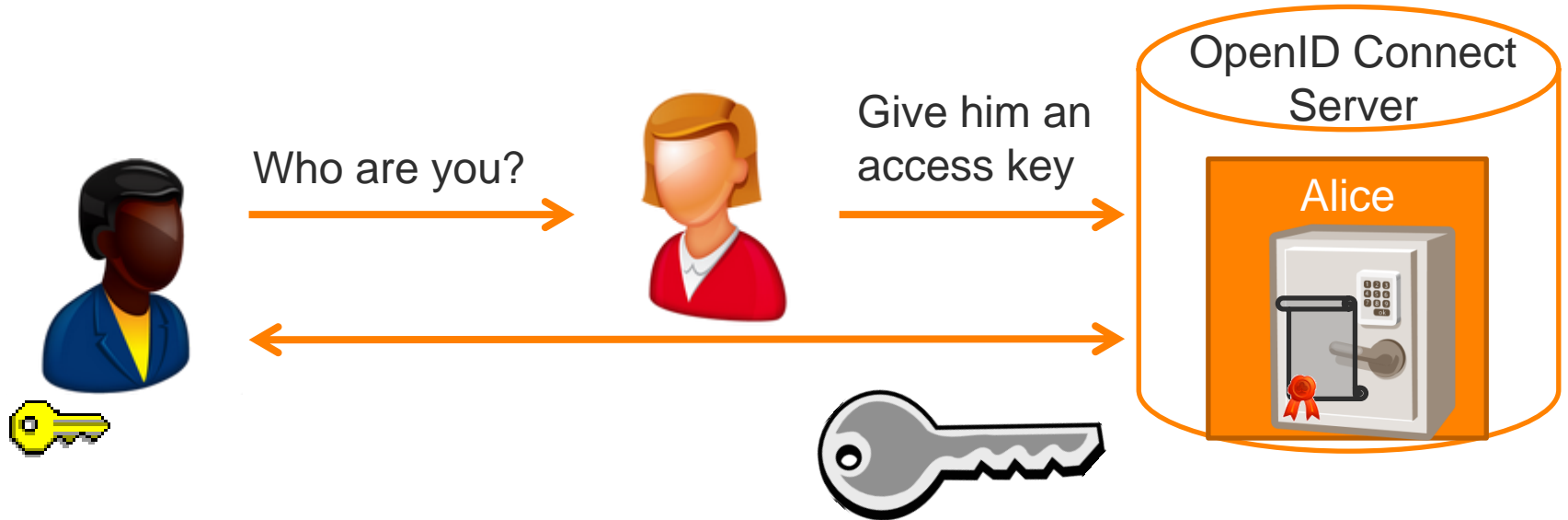
USA TODAY and Google will use this information in accordance with their conditions and their respective privacy policies.

Cancel I agree



OAuth Authorization





Define YOUR solution

- ✦ Confidentiality / Personal data sharing?
- ✦ Pre-registration of web application?
- ✦ Dependency to an identity provider?
- ✦ Authentication methods?

THE Message

- ✦ Passwords are bad
 - ✦ Strong Authentication
- ✦ Too many identities is inconvenient
 - ✦ Reuse identities (emails, social networks...)
- ✦ Authentication is a sensitive and potentially complex task
 - ✦ Delegation, SSO
- ✦ Privacy needs to be protected
 - ✦ Don't ask for more data or access rights than needed

Thanks