OpenID Connect

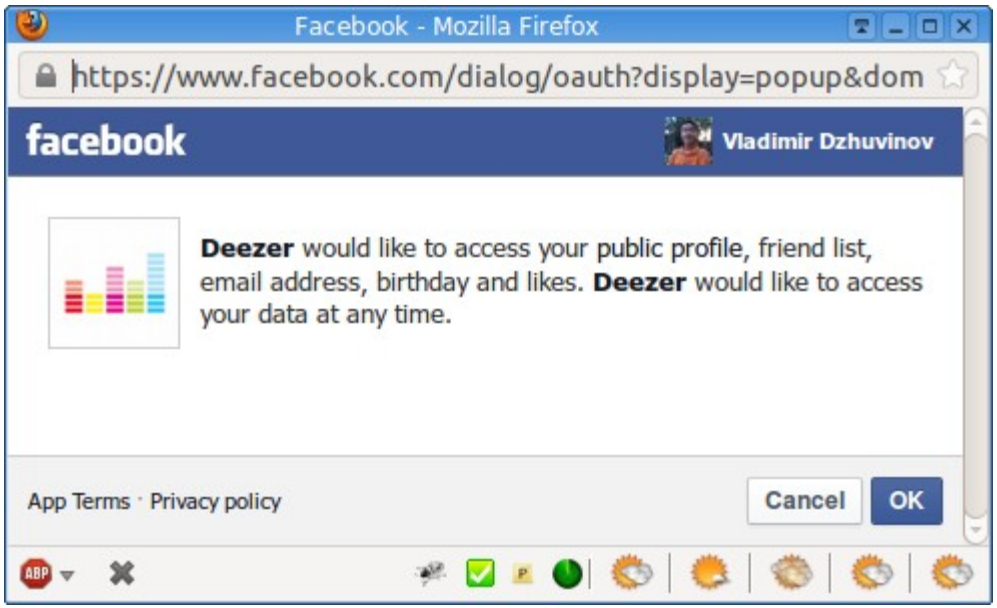
Как да си върнем личната идентичност в мрежата

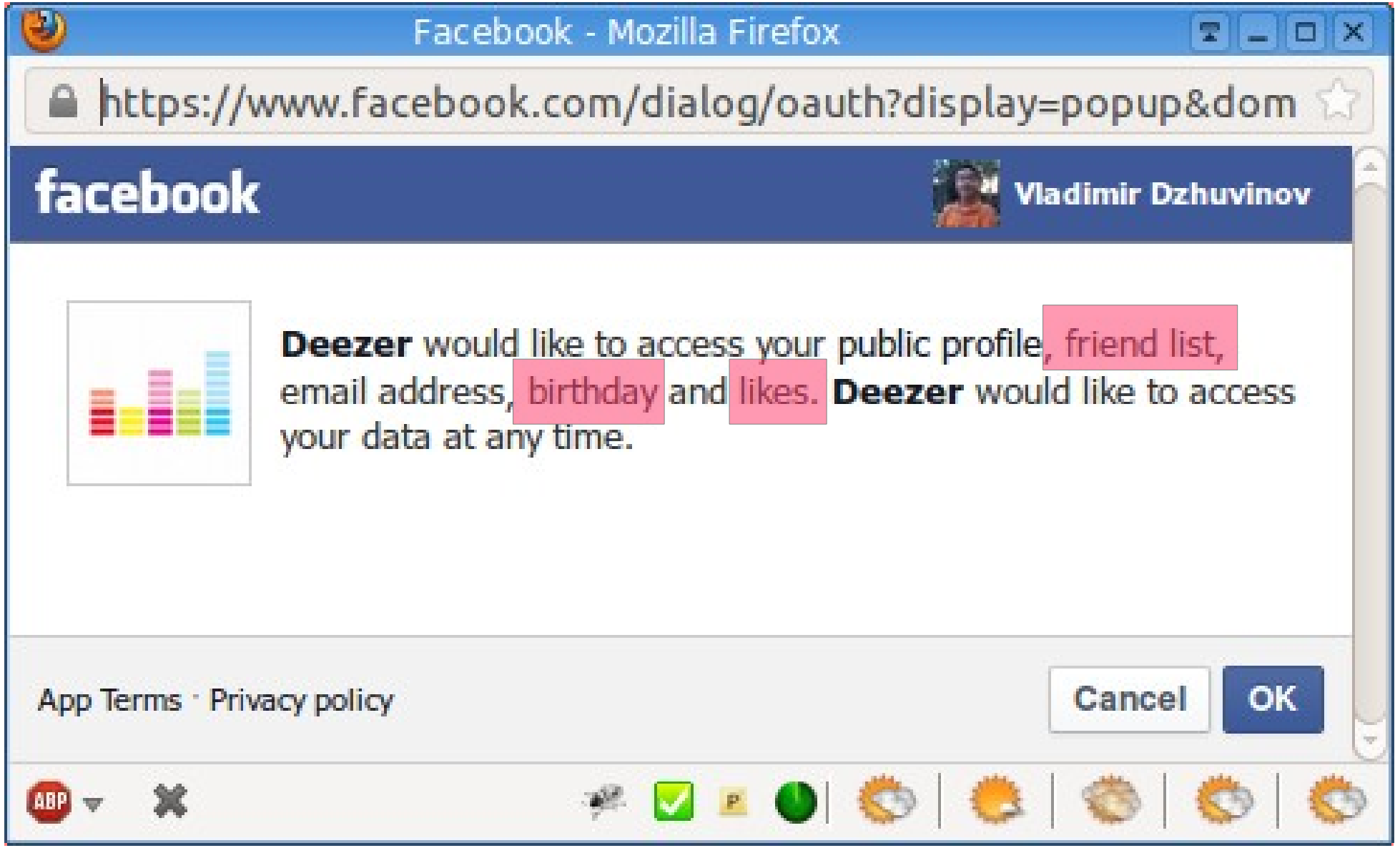
Владимир Джувинов | NimbusDS.com | PlovdivConf | 6 юли 2013

@dzhuvinov

- NimbusDS - web IdM, SaaS user onboarding
- WG:
  - OpenID Foundation, Connect A/B
  - IETF OAuth
  - IETF JavaScript Object Signing and Encryption (JOSE)


Велоклуб
КРИВА СПИЦА
www.kriva.org

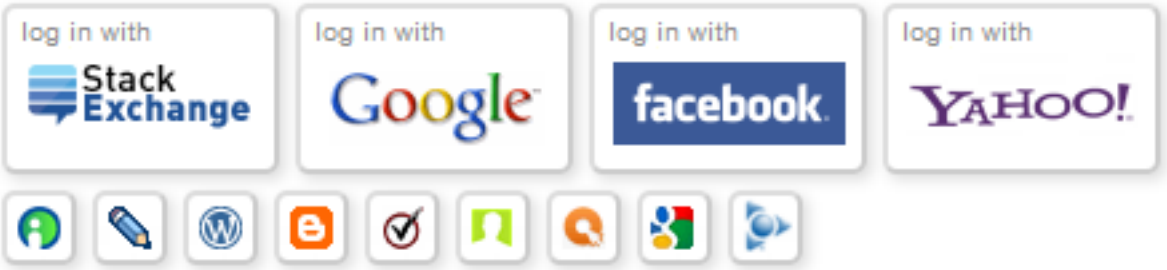

Facebook - Mozilla Firefox
https://www.facebook.com/dialog/oauth?display=popup&dom
facebook
Vladimir Dzhuvinov
Deezer would like to access your public profile, friend list, email address, birthday and likes. Deezer would like to access your data at any time.
App Terms · Privacy policy
Cancel
OK


Facebook - Mozilla Firefox
https://www.facebook.com/dialog/oauth?display=popup&dom
facebook
Vladimir Dzhuvinov
Deezer would like to access your public profile, friend list, email address, birthday and likes. Deezer would like to access your data at any time.
App Terms · Privacy policy
Cancel
OK

Questions Tags Tour Users

Log In

Do you already have an account on one of these sites? Click the logo to **log in** with it here:



Тази лекция

- Системните проблеми на удостоверянето днес
- Поуките зад OpenID Connect
- Един бутон за вход за всички
- Демократизация на удостоверяването
- Групова молитва всичко това да се случи :)

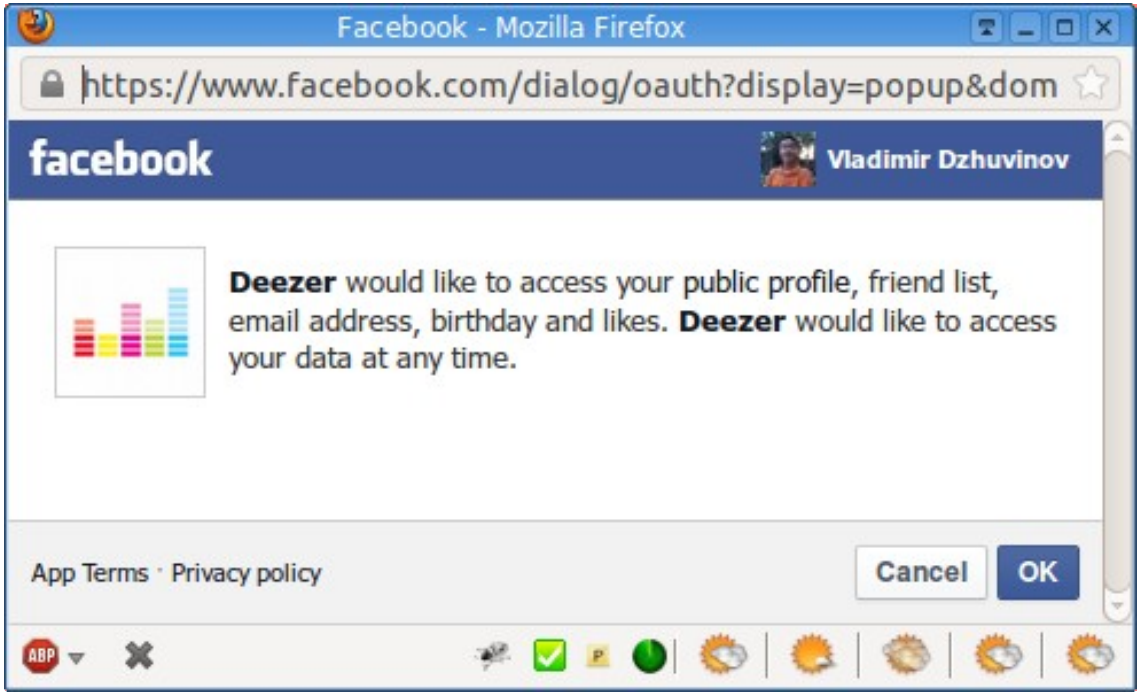
Мащабно концентриране на профили и удостоверяване

Шепа компании държат глобалното удостоверяване като услуга в интернет: Facebook, Google, Twitter, Yahoo...

Следене и събиране на данни

Концентрирането на потребителските профили и login към приложенията на едно място прави следенето много лесно

Лични данни



В повечето случаи нямаме избор да откажем достъпа до определени наши лични данни

OK / Cancel

Общоприет удостоверителен протокол

Такъв на практика все още липсва.

Всеки IdP изисква собствен Login/SSO протокол, и интегрирането на специфична библиотека.

Ни дава път за системното решаване на всички тези проблеми

Оригиналният OpenID vs OAuth

Какво прави влизането с авторизационния протокол OAuth по-атрактивно за клиентските сайтове и самите IdP?

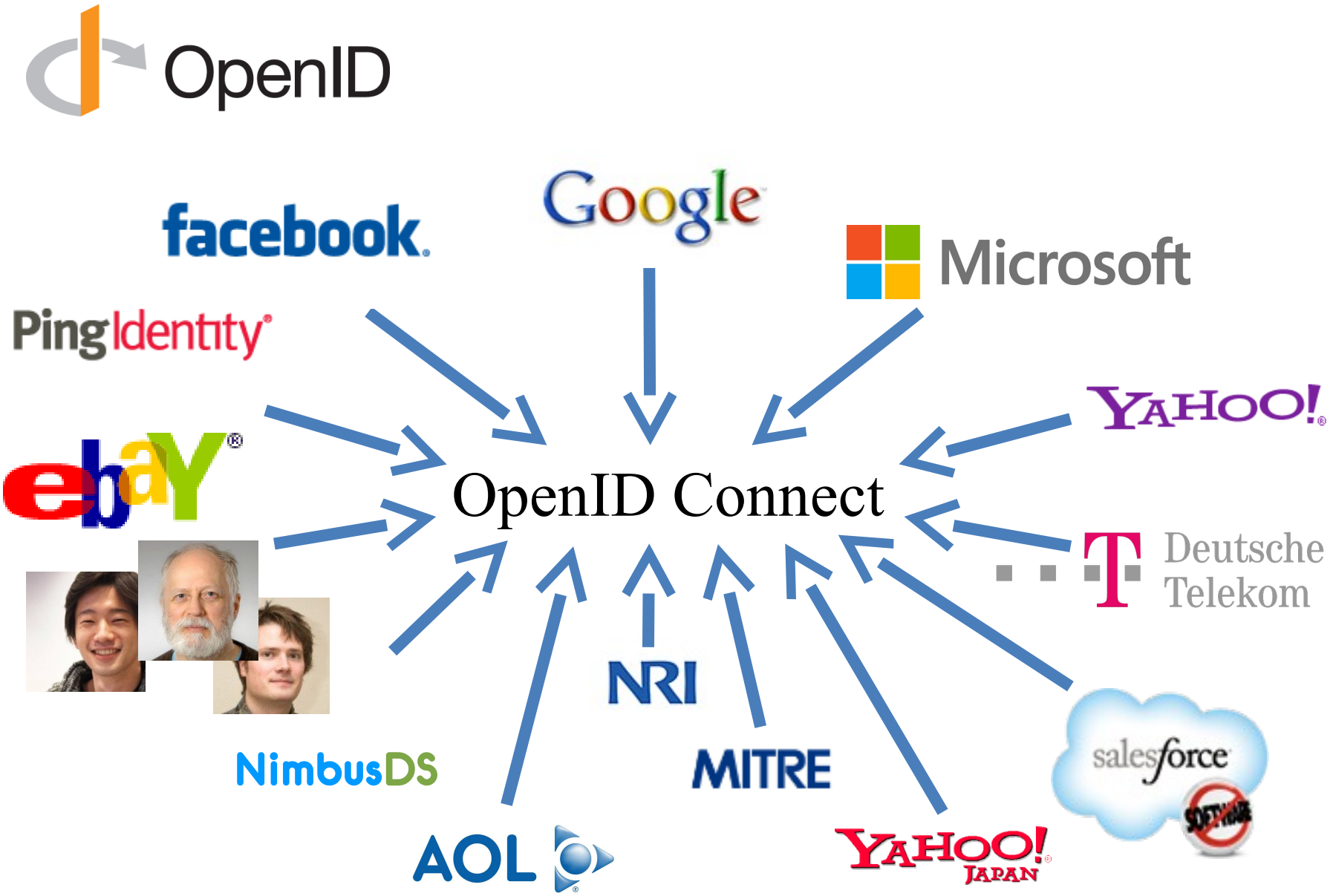
FB OAuth, Google OAuth, Twitter OAuth, и др. предоставят:

1. **Удостоверяване**

2. **Жетон (token) за достъп до user info и API на свързаното приложение**

Уроците зад OpenID Connect

- **Трябва да бъде и авторизационен протокол:** потребителят да може да издава жетон (token) за достъп до определени приложни API от негово име
- **Трябва да дава възможност за автоматично откриване на IdP на потребителя:** шанс за “второразрядни” компании в интернет, на които не биха им сложили “Login with me” бутона

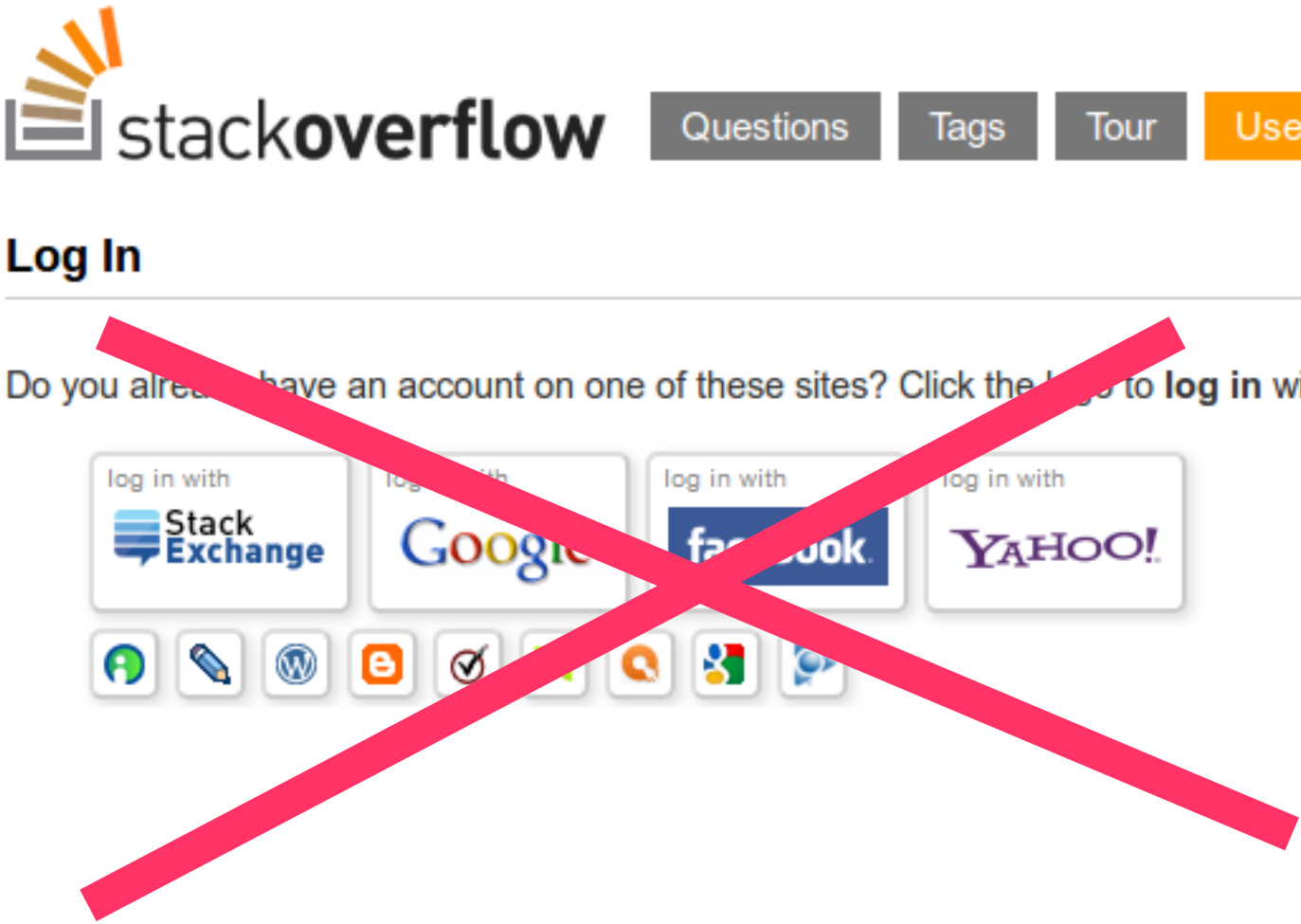

OpenID
facebook
Google
Microsoft
PingIdentity
YAHOO!
ebay
OpenID Connect
Deutsche Telekom
NRI
NimbusDS
MITRE
salesforce
AOL
YAHOO! JAPAN

OpenID Connect

- Базиран на OAuth 2.0
- Издава:
  - ID token
  - access/refresh token
- Автоматично откриване (Discovery)
- Автоматична регистрация
- Self-issued IdP
- Поддържа web, native + mobile приложения

Discovery / Web Finger

- Протокол за откриване на **IdP** на даден потребител по email адрес
- Подобен на Unix finger ;-)
- **“Твърдото връзване” между клиентски сайт / приложение и IdP вече не е нужно!!!**
- **Демократизация на IdP услугите**


stackoverflow
Questions
Tags
Tour
Users
Log In
log in with
Stack Exchange
log in with
YAHOO!

Questions Tags Tour Users

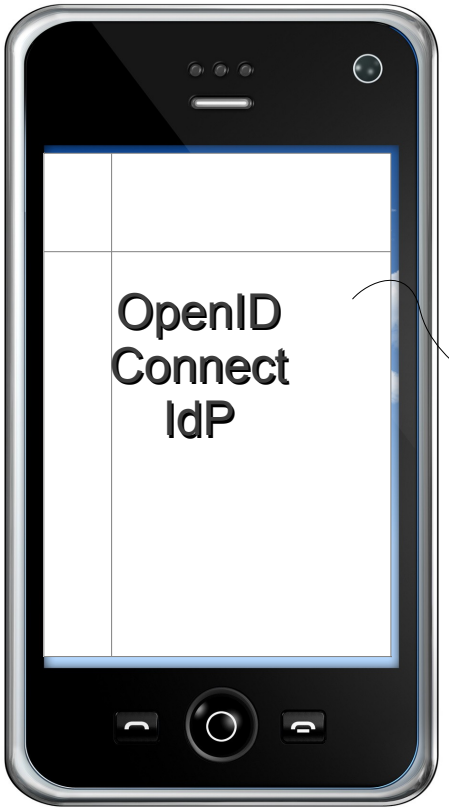
Log In

vladimir@nimbusds.com

Self-Issued

- Дава възможност на всяко лице да бъде **OpenID Connect IdP за себе си**
- **“Аз съм аз”**
- По подобие на self-signed / root SSL сертификатите
- Всеки смартфон или браузър може да стане **IdP за неговия притежател**

Self-Issued IdP in Smartphone



“Аз съм Владо,
trust me!”

Вашите лични данни и профил стоят само във вашия смартфон.

Влизате и се удостоверявате в приложения направо чрез него.

Self-issued IdP in Browser

Пример:

OpenID Connect Self-Issued IdP
като Firefox Add-on:

Пази вашите лични данни вътре в браузъра.

Използвате вашия личен браузър за удостоверяване и влизане в приложения.

Търсят се доброволци за създаването на такъв Add-On!

Пътна карта

- OpenID Connect статус: 2nd implementer's draft
- Очакван стандарт 2014
- IETF OAuth
- IETF Javascript Object Signing and Encryption (JOSE)
- Все още има много работа, вкл. по InterOp

Java OpenID Connect библиотеки

от NimbusDS

За повече инфо:
http://openid-connect.info

 # Nimbus OAuth 2.0 SDK with OIDC ext

 # Nimbus JOSE+JWT

 # Nimbus LangTag

Q + A