

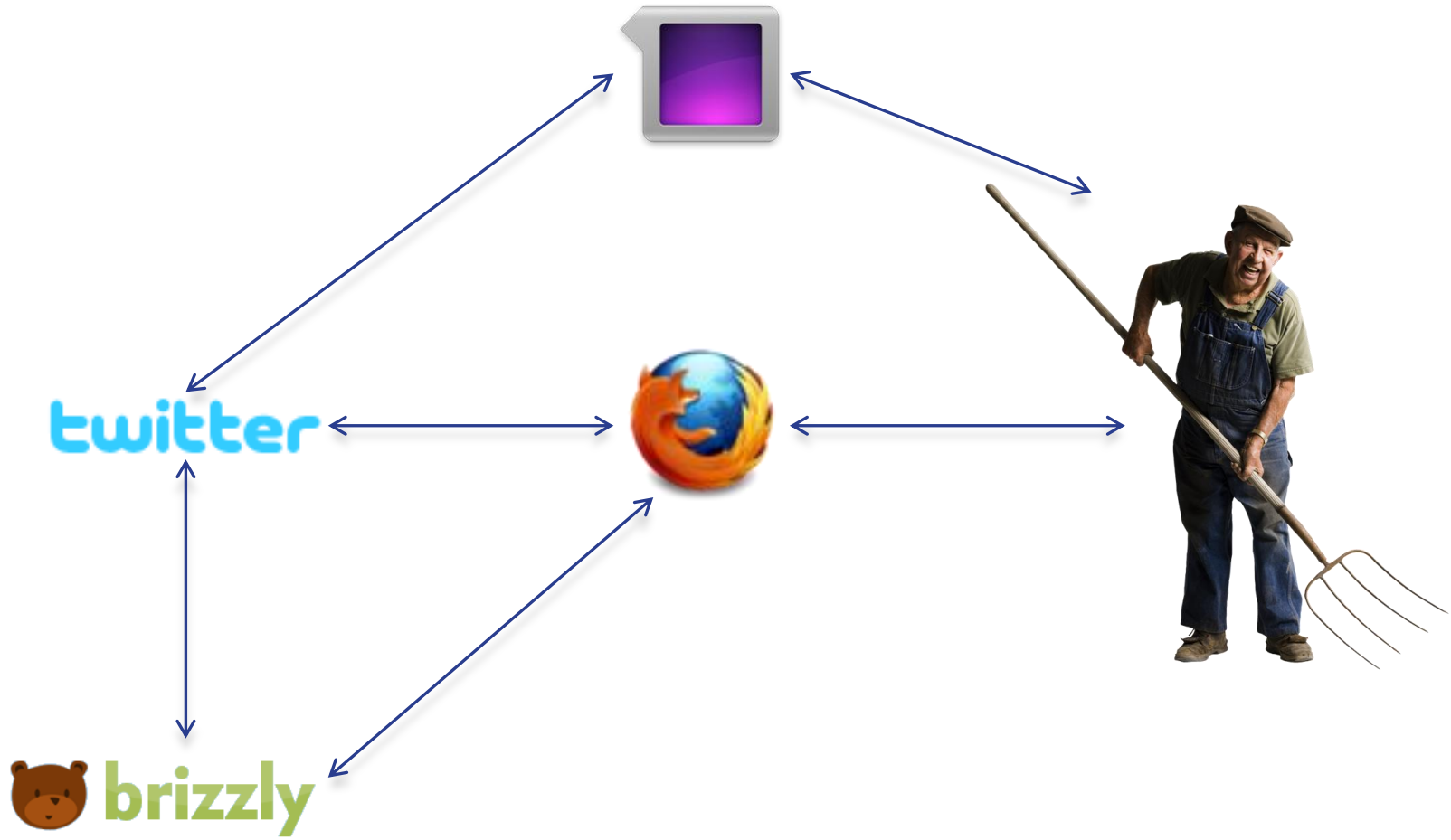


Martin Matula ([martin.matula@oracle.com](mailto:martin.matula@oracle.com))

28.2.2011, Setkání pražského CZJUG

- \* Úvod - webové služby a autentizace
- \* Co je OAuth
- \* Ukázka OAuth klienta a serveru
- \* OAuth.next stručně
- \* Nabídka práce, Q&A, občerstvení

 **Agenda**



- \* Mnoho hojně používaných webových aplikací zveřejňuje API pro vývojáře
  - \* Twitter, Facebook, Google Apps, atd.
- \* V drtivé většině populárních webů převažuje jednoduché HTTP API (v ideálním případě RESTful) nad SOAP WS

# \* Webové služby a REST

- \* Autentizuje se koncový uživatel svými credentials
  - \* Jméno a heslo  
(HTTP Basic Auth., HTTP Digest Auth.)
  - \* Certifikát
- \* Vyžaduje vysokou míru důvěry koncového uživatele vůči klientské aplikaci
- \* Funguje dobře pro webové aplikace - uživatelé důvěřují webovým prohlížečům

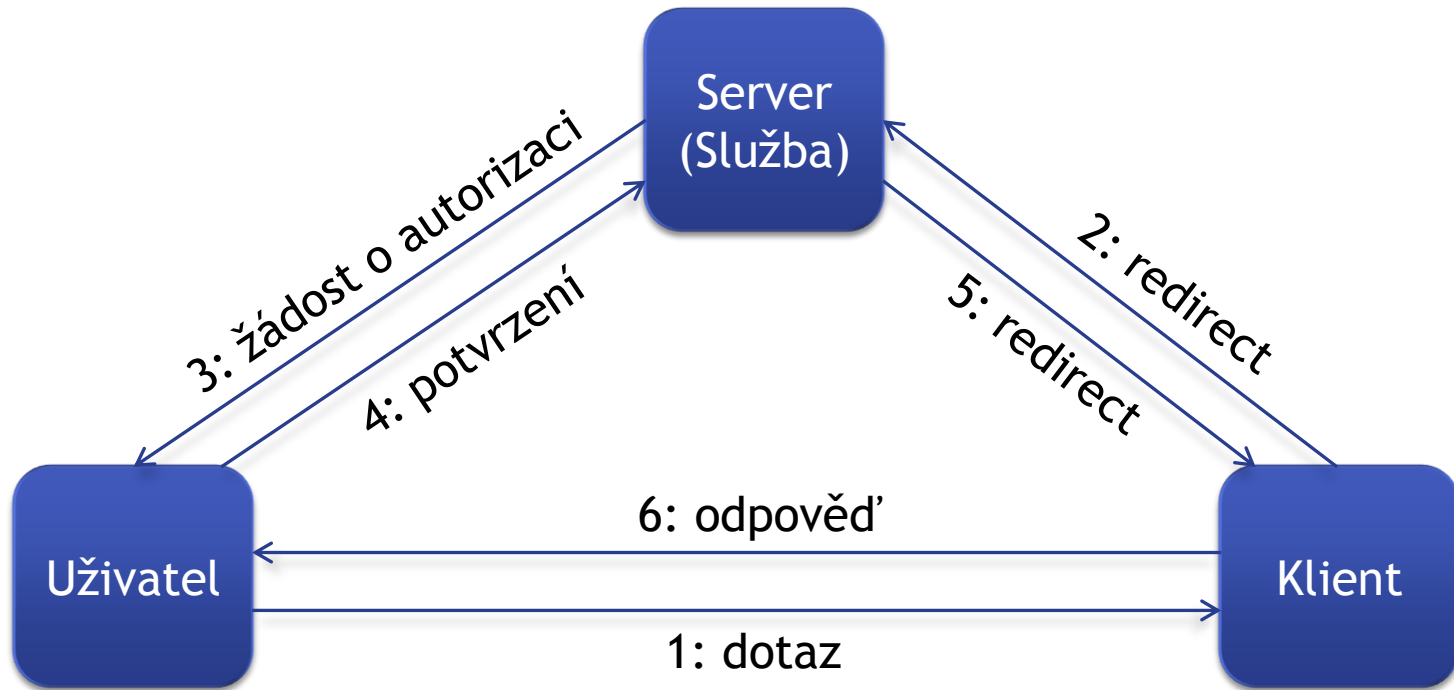
## \* Klasická autentizace

- \* Sdílení uživatelských credentials s klientskou aplikací je nežádoucí
  - \* Poskytuje plnou autoritu klientské aplikaci
  - \* Nelze spolehlivě odebrat přístup pro daného klienta
- \* Vznikla řada řešení od různých firem
  - \* Amazon Signature, Google AuthSub, Yahoo BBAuth, Microsoft Shared Key, ...
- \* OAuth se stává v této oblasti standardem

# \* Autentizace a webové služby

- \* An open protocol to allow secure API authorization in a simple and standard method from desktop and web applications
- \* Komunitní verze - OAuth Core 1.0 a 1.0a
- \* Později nahrazeny RFC 5849 - IETF OAuth 1.0
- \* Umožňuje aplikacím přístup k chráněným prostředkům ve jménu uživatele bez potřeby znalosti uživatelských credentials

\* OAuth 1.0



# \* Autorizační “flow”

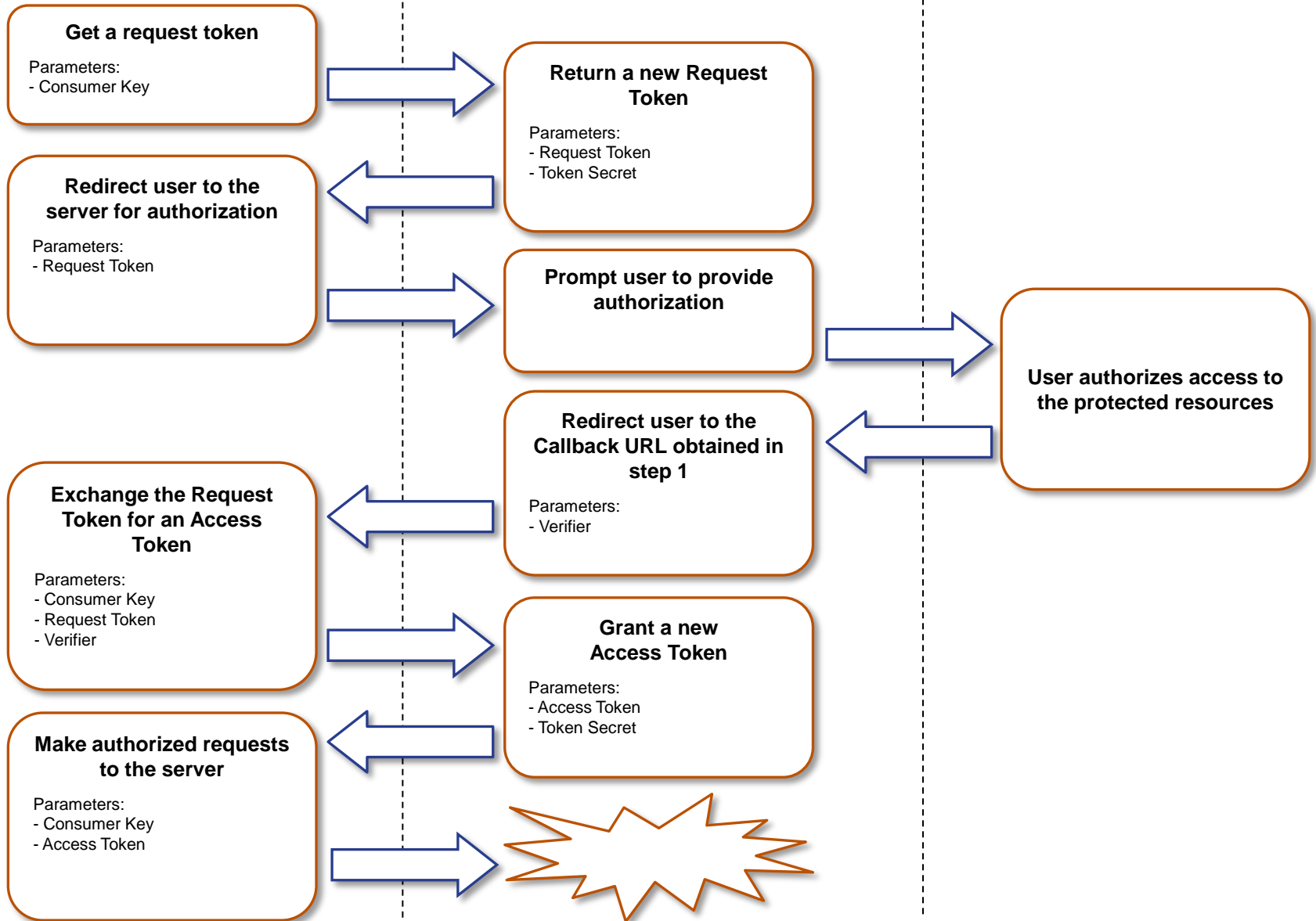
- \* Používá klientské credentials pro autentizaci klientské aplikace
  - \* Consumer Key, Consumer Secret
- \* Přístupový token pro ověření autorizace
  - \* Access Token, Token Secret
- \* “Secret” část se neposílá po drátě - používá se pouze k podpisu zpráv
  - \* Nevyžaduje použití SSL k ochraně credentials

## \* OAuth 1.0 v detailu

## Client

## Server

## User



- \* Jersey (<http://jersey.java.net>)
  - \* Framework pro vývoj RESTových služeb v Javě
- \* Implementace standardu JAX-RS
- \* Řada dalších “value-add” funkcí
  - \* Klientské API, podpora WADL, MVC, atd.
- \* Podpora OAuth 1.0 na klientské i serverové straně



## \* OAuth a Jersey

- \* Implementován jako klientský filtr
- \* Automaticky podepisuje odchozí zprávy dle nastavených klientských credentials a přístupového tokenu
- \* Výrazně zjednodušuje implementaci autorizačního flow
- \* Maven modul oauth-client
  - \* GroupId: com.sun.jersey.contribs.jersey-oauth

## \* Jersey OAuth klient

- \* Implementuje filtr na straně serveru, který verifikuje OAuth hlavičky v příchozích zprávách
- \* Vydávání request a access tokenů
- \* Správa tokenů a klientů je specifická pro každou aplikaci - zasouvá se implementací SPI
  - \* Modul obsahuje default implementaci pro testovací účely
- \* Maven modul: oauth-server
  - \* GroupId: com.sun.jersey.contribs.jersey-oauth

## \* Jersey OAuth server

Yammer

photobucket

NETFLIX

IRON MONEY

opensocial

echowaves

twitter

ohloh:

cliqset

TripIt Organize your travel

Google

Agree 2

88 MILES

smart.fm

YAHOO!

meetup

vimeo

myspace.

EVERNOTE

tarpipe

SmugMug

fire eagle

get satisfaction

PRAIZED

# \* Rozšířenost OAuth 1.0

- \* OAuth 1.0 má své problémy
  - \* Správná implementace podpisů je netriviální
  - \* Úzké propojení mezi primární a autorizační funkcionalitou služby
  - \* Zbytečné zatížení na straně serveru
  - \* Obtížnější implementace newebových klientů
- \* OAuth WRAP
- \* OAuth 2.0

## \* Budoucnost OAuth

- \* WRAP = Web Request Authentication Protocol
- \* Google, Yahoo a Microsoft
- \* Pokus o řešení problémů s OAuth 1.0
- \* Přináší podporu více profilů/use-casů
  - \* Desktopové aplikace, JavaScript klienti
  - \* Web profile flow stejné jako u OAuth 1.0
- \* Místo podpisů používá SSL
- \* Vstup pro OAuth 2.0

## \* OAuth WRAP stručně

- \* Momentálně ve vývoji jako standard v rámci OAuth WG v IETF (nyní draft #13)
- \* Nekompatibilní s OAuth 1.0
- \* Jednoduchý
  - \* Odbourána nutnost implementace podpisů,
  - \* Zjednodušené autorizační flow pro různé typy klientů
- \* Lepší výkon a škálovatelnost
  - \* Zjednodušený state-management během autorizace
  - \* Oddělení autorizačních a resource serverů
- \* Formalizovaná rozšiřitelnost
  - \* Registr typů tokenů, registr OAuth parametrů, ...

## \* OAuth 2.0 stručně

- \* OAuth 1.0 - Otevřený standard
- \* Podpora množství firem
- \* Funguje na základě klientských credentials, přístupových tokenů a podpisů
  - \* Uživatel nemusí odkrývat své credentials
  - \* Přístup lze kterémukoliv klientovi odejmout
- \* Nevyžaduje SSL
- \* V Javě se implementace výrazně zjednodušuje použitím OAuth podpory v Jersey
- \* Dalším vylepšením bude OAuth 2.0, který ale momentálně není hotový

\* Závěr

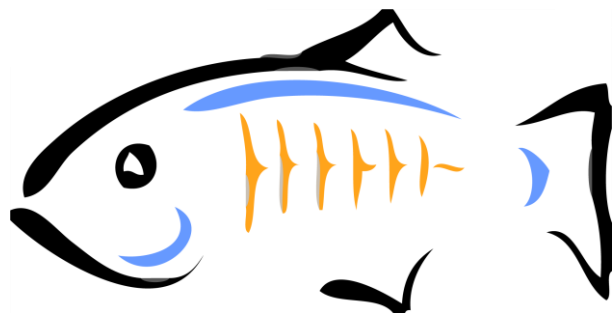
\* Užitečné odkazy

\* OAuth - <http://oauth.net>

\* Jersey - <http://jersey.java.net>

\* Pojd'te k nám pracovat!

\* CV pošlete na [martin.matula@oracle.com](mailto:martin.matula@oracle.com)



\* **Dotazy?**