

### **FORGEROCK**<sup>™</sup>

## An Introduction to User-Managed Access (UMA)

Eve Maler VP Innovation & Emerging Technology eve.maler@forgerock.com \$\complex.mlgrrl

October 22, 2014

# Challenges in apps that handle personal data and content





# Some apps are still in the Web 1.0 dark ages

- Provisioning user data by hand
- Provisioning it by value
- Oversharing
- Lying!

| Name           |                  |
|----------------|------------------|
| Street Address |                  |
|                |                  |
| City           |                  |
| State          | Enter Text       |
| Zip/Postal     |                  |
| Province       |                  |
| Country        | Enter Text       |
| Phone          |                  |
| Email          |                  |
| Preferred      | O Postal Mail    |
| Communication  | Phone     F-mail |
|                |                  |



# Some other apps are still in the Web 2.0 dark ages

| <ul> <li>Mint®: Money, Budgeting, Finance &amp; Investing</li> </ul> |   | R <sub>M</sub> |
|--|---|----------------|
| <   > 🛆 🖻 🥵 🔆 / + 🖉 INTUIT INC. 🕯 www.mint.com 🖒                     |   |                |
| 1  | Mint®: Money, Budgeting, Finance & Investing  | +              |
| <b>Emint</b> .com  | Email     Password     & Log in     & Sign up       WHAT IS MINT?     HOW IT WORKS     FIND SAVINGS     COMMUNITY     COMPANY |                |

## It's easy to understand what's going on with your money.

Get a handle on your finances the *free* and fast way. Mint does all the work of organizing and categorizing your spending for you. See where every dime goes and make money decisions you feel good about.

New! Mint now offers truly free credit scores right inside Mint. No credit card required. Learn More

The "password anti-pattern" – a third party impersonates the user

 It's a shared secret honeypot

×

 It's a gray-market B2B partner



## Apps using OAuth and OpenID Connect hint at a better, if not perfect, way





## Apps using OAuth and OpenID Connect hint at a better, if not perfect, way



#### 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.
- Access your direct messages.

#### Authorize app

This application will not be able to:

· See your Twitter password.

You can revoke access to any application at any time from the Applications tab of your S By authorizing an application you continue to operate under Twitter's Terms of Service. I

Cancel

 Image: Second state of the second s

usage information will be shared back with Twitter. For more, see our Privacy Policy.



By Meshfire www.meshfire.cc Ignite your comn

Meshfire



**Lwitter** 

 $-\frac{1}{2}$ 

### An application would like to connect to your account

The application **KanyeAnalysis**<sup>™</sup> by **imma-let-u-finish** would like the ability to **access and update** your data on Twitter. This application also plans to **murder all of your children**.

#### Allow KanyeAnalysis<sup>™</sup> to murder your children?





# What about selective person-to-person sharing?

|   | Vancouver, WA, September 2014   |  |  |  |
|---|---|--|--|--|
|   | Sep 24 - 26, 2014 / Vancouver, WA   |  |  |  |
| Travelers: Eve L Maler V Add  |   |  |  |  |
|   | Viewers: Add Planners: Add  |  |  |  |
| A C C   |   |  |  |  |
| Here Comes the Sun choreo – Google Docs   |   |  |  |  |
| Here Comes the Sun choreo – Google Docs +   |   |  |  |  |
| Here Comes the Sun choreo       Image: migrrl@gmail.com         File       Edit       View       Insert       Format       Tools       Table       Add-ons       Help       Last edit was made on August 19, 2013 by Mindy Engelberg       Comments       Image: mindpart |   |  |  |  |
|   | Image: More in the image: Second interval and the image: Secon |  |  |  |





# Our choices: send a private URL...

- Handy but insecure
- Unsuitable for really sensitive data





## Or implement a proprietary access management system...

Sharing settings Link to share (only accessible by collaborators) https://docs.google.com/document/d/1ISWPDnkck1K\_epT4fJTj2EjEWfzEoCKzoOSM& М 🚺 🖬 🔰 Share link via: Who has access Specific people can access Change... Eve Maler (you) xmlgrrl@gmail.com Å Is owner Kat E Can edit -× Is owner Mindy Engelberg Can edit Can comment Can view Invite people: Enter names or email addresses... Editors will be allowed to add people and change the permissions. [Change] Done



## Or require impersonation

## Import Fidelity Tax Information Into TurboTax®

If you are a Fidelity customer and use TurboTax<sup>®</sup>, you may be able to import certain information directly from your account into the software. Here's how.

#### How to import your information

Once you receive your 1099 statement by mail or through eDelivery, have it available to verify the imported information. Follow these simple steps:

 Enter your Social Security number (SSN), taxpayer identification number (TIN), or username, and then your password. When asked where to import information from, select Fidelity Investments and enter the same information that you use to log on to Fidelity.com. Then, the tax information available for each of the accounts associated with your SSN should appear.



## Killing – or even *wounding* – the password kills impersonation





# We have tough requirements for delegated authorization

- Lightweight for developers
- Robustly secure
- Privacy-enhancing
- Internet-scalable
- Multi-party



Enables end-user convenience



## Introducing UMA





## **UMA in a nutshell**



- It's a draft standard for "authorization V.next"
- It's a profile and application of OAuth V2.0
- It's a set of authorization, privacy, and consent APIs
- It's a Work Group of the Kantara Initiative
- It's not an "XACML killer"
- Founder, chair, and "chief UMAnitarian":



It's heading to V1.0 in Q1 2015





# The UMA protocol enables key new use-case options











## **Use-case scenario domains**

Health

Financial



Education















# UMA-enabled systems can respect policies such as...

Only let my tax preparer with email **TP1234@gmail.com** and using client app **TaxThis** access my **bank account data** if they have **authenticated strongly**, and **not after tax season is over**.

Let my health aggregation app, my doctor's office client app, and the client for my husband's employer's insurance plan (which covers me) get access to my wifi-enabled scale API and my fitness wearable API to read the results they generate.

When a person driving a vehicle with an **unknown ID** comes into contact with my **Solar Freakin' Driveway**, alert me and **require my access approval**.



The user experience can simulate **OAuth or** proprietary sharing paradigms, or even be invisible ("better than **OAuth**")

#### Sharing settings

#### Link to share (only accessible by collaborators)

https://docs.google.com/document/d/1ISWPDnkck1K\_epT4fJTj2EjEWfzEoCKzoOSM{

| Share link via: 💽 🚺 丁 |  |                         |  |
|-----------------------|--|-------------------------|--|
| Who I                 | has access                                     |                         |  |
| -24                   | Specific people can access                     | Change                  |  |
|                       | Eve Maler (you) xmlgrrl@gmail.com              | Is owner                |  |
|                       | Kat E  | Can edit - ×            |  |
| 5                     | Mindy Engelberg                                | ls owner<br>✓ Can edit  |  |
|                       |  | Can comment<br>Can view |  |
| Inv<br>E              | vite people:<br>Inter names or email addresses |                         |  |

Editors will be allowed to add people and change the permissions. [Change]

Done



## Under the hood, it's "OAuth++"



# The UMA consent model supports robustly partitioned rights and obligations





# The UMA consent model supports robustly partitioned rights and obligations



**FORGEROCK**<sup>TM</sup>



### FORGEROCK

## Thank you!

Eve Maler VP Innovation & Emerging Technology eve.maler@forgerock.com \$`@xmlgrrl

FORGEROCK.COM

## Appendix: The gory UMA details













#### The AS exposes an resource UMAowner manage consent standardized control authorization negotiate protect resource requesting authorization server party server **API** to the Authorization API client Authorization request endpoint authorization API token AAT authorize access manage The AAT protects the API Authorization client and binds the RqP, client, and AS client The client may be told:

"need\_claims"



# The AS can collect requesting party claims to assess policy



