

Public Design

a discussion of the oauth standards process

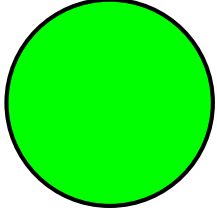
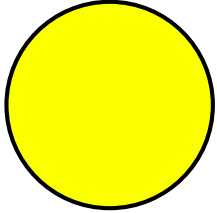
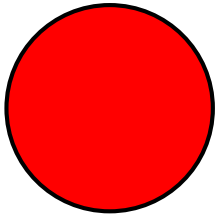
Blaine Cook

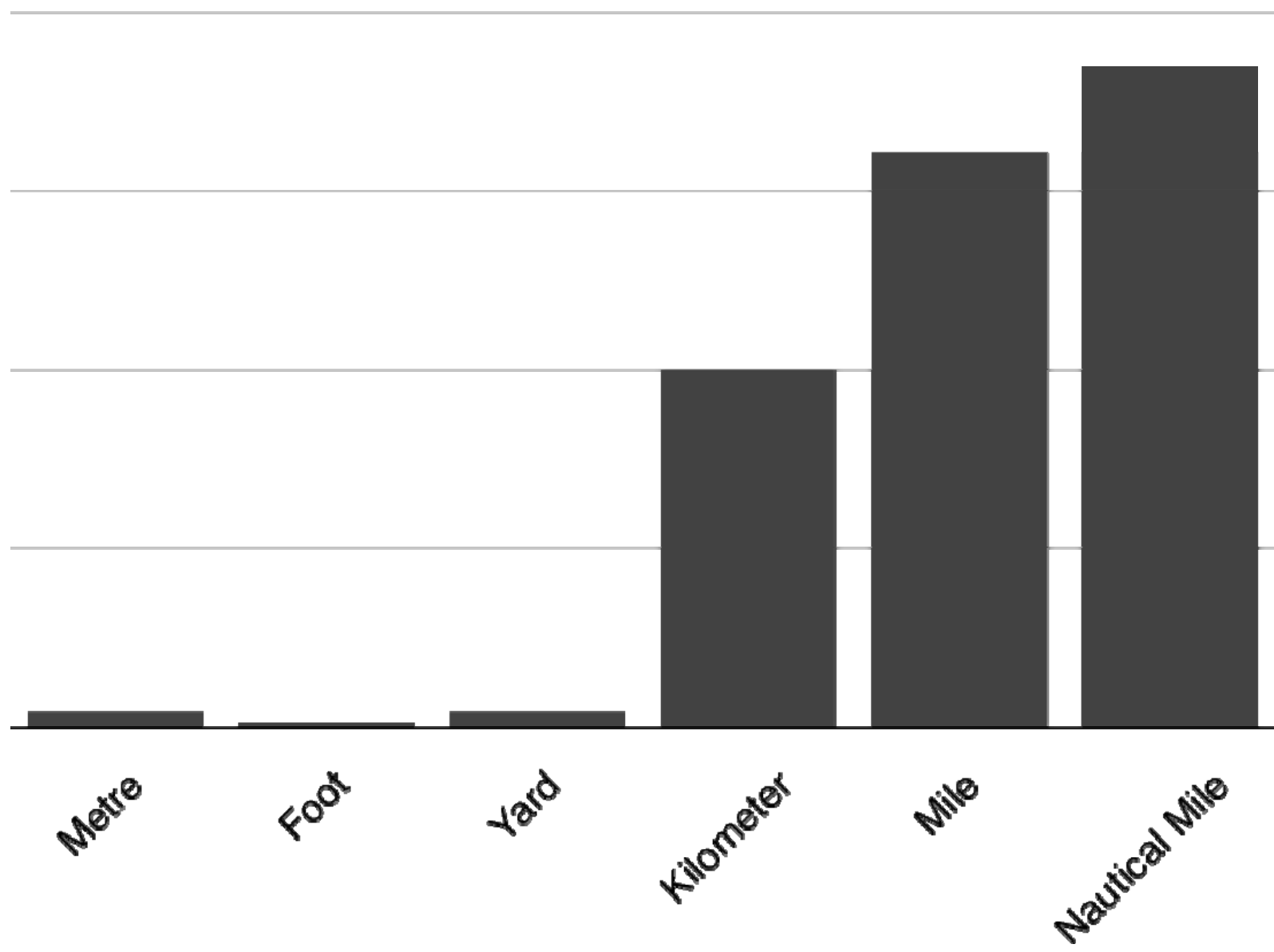
Twitter, Inc.

*“Don’t re-invent
the wheel.”*

*“If it ain’t broken,
don’t fix it.”*

Standards





OAuth

(a brief introduction)

“OAuth is your valet key for the web.”

Eran Hammar-Lahav

OAuth Specification Editor

“OAuth is a standard that defines a secure mechanism for providing delegated authentication via the web. It enables users of a service to grant access to third parties to act on their behalf, without divulging their identity or credentials.”

“OAuth is a **standard** that defines a **secure** mechanism for providing delegated **authentication** via the web. It enables users of a service to grant access to third parties to act on their behalf, without divulging their identity or credentials.”

Process

Building a better wheel, together.

OAuth isn't novel.

- Flickr Auth
- Google AuthSub
- Yahoo BBAuth
- Amazon AWS Auth
- AOL OpenAuth
- etc.

Primary Goals

- Extraction of an existing pattern
- Clear use cases
- Secure, given the threat model
- As simple as possible
- Easy to implement
- And therefore easy to adopt

Share.

- Security through obscurity doesn't work
- Adoption won't happen without consensus
- Involve interested parties
- ... if they agree to the primary goals
- Ensure their voice is heard
- Generate a first draft
(Request For Comments)

Listen.

- What are some of the use cases you didn't imagine?
- What are the problems thus far?
- Is there interest?

Build Consensus.

- Incorporate feedback into a new draft
- Even better, encourage contributors to change the draft themselves
- Facilitate, ensure primary goals are being met

Peer Review

- Is it correct?
- Are the initial goals still met?
- Experiment with implementations
- Fix known problems
- Invite many reviewers

Ship It!

iterate as necessary

Open Source

- libraries in perl, python, C++, ruby, javascript, others
- built on pre-existing cryptographic libraries (openssl, hmac-sha1)

Adoption

(since release on Dec. 04 2007)

- Google (OpenSocial)
- Yahoo! (BravoNation, “Fire Eagle”)
- MySpace
- Mag.nolia
- Pownce, Jaiku, Twitter
- NetFlix
- Digg, Flickr, SixApart, Blogger expected