Safe Single Sign-On for the RJI Information Trust Exchange

September 28 2015 / By Drummond Reed

Material: Added by Bill Densmore

Introduction

The RJI Information Trust Exchange (ITE) will create a new ecosystem for news in which producers of original content can be rewarded for the value of that content no matter where it is syndicated, and consumers of that content can easily access and pay for it no matter where it is syndicated (directly, via subscription, or via sharing of user attributes and attention that can be monetize through advertising).

The hallmark of the ITE ecosystem is **lower friction**:

1. Lower friction for ethical content syndication
2. Lower friction for content access
3. Lower friction for user attribute exchange
4. Lower friction for payment

If the ITE can lower friction along each of these four dimensions, everyone wins.

The first of these four dimensions—ethical content syndication—is a B2B process between content providers. Lowering friction on this dimension requires a combination of technical and business agreements for attribution and compensation.[1]

Lowering friction along the other three dimensions—content access, user attribute exchange, and payment—requires lowering friction for end-users.

Social Login

The best example of how such end-user friction has been lowered in the past decade is **social login**. The term applies to the buttons that enable members of social networks like Facebook, Twitter, LinkedIn, or Google

[1] The combination of technical standards with business, legal, and policy agreements for using these standards is called a *trust framework*. Trust frameworks are a major new area of Internet innovation. See the Open Identity Exchange, http://www.openidentityexchange.org/.

to register or login at websites or mobile apps with as little as one click without having to create a new username or password. Figure 1 illustrates the basic flow of social login.

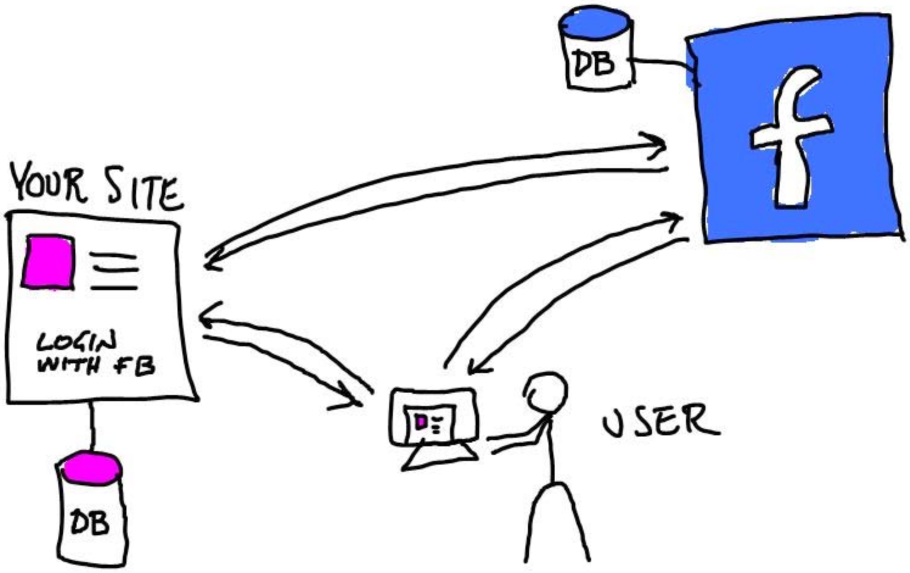


Figure 1: How Social Login Works

Figure 2 provides a more detailed flow diagram of social login—specifically how it works with a mobile app in addition to a browser.

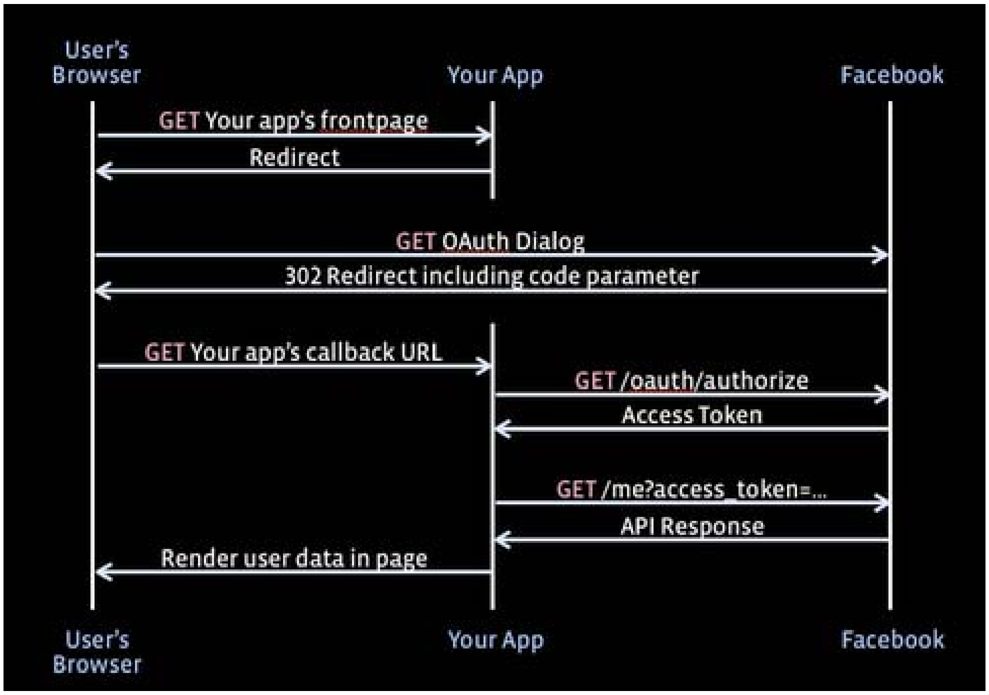
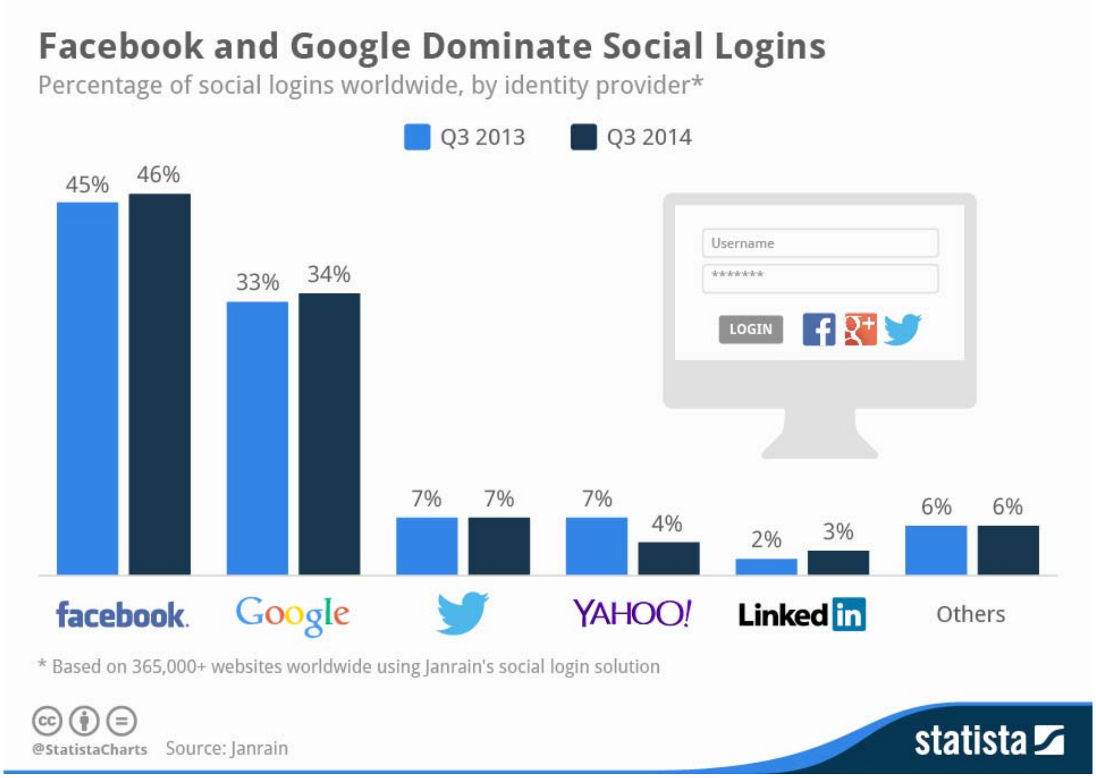


Figure 2: Technical Summary of Social Login Flow

When first introduced, social login proved very popular with both websites and users. Facebook and Google now dominate the social login market. Figure 3 shows the current market shares worldwide.



Facebook and Google Dominate Social Logins

Percentage of social logins worldwide, by identity provider*

* Based on 365,000+ websites worldwide using Janrain's social login solution

Source: Janrain

Figure 3: Social Login Market Shares

However, despite its enormous advantages in convenience and usability, in 2014 the growth of social login began to “hit the wall” of privacy and trust issues. To wit:

1. Users became concerned about how much of their data was being shared by the social networks wanted to start keeping their web activity separate.
2. Websites became concerned about the privacy implications of social login and about having intermediary between them and their users.

For both reasons major websites such as the *New York Times* began removing social login buttons, and other sites have become much more careful about when and where they are allowed.

Safe Single Sign-On

In the past two years, an alternative to social login has emerged called **safe single sign-on**. The term was coined by Doc Searls, a leader in the new field of Vendor Relationship Management (VRM) —where customers have the same tools for managing vendor relationships that vendor use for Customer Relationship Management—CRM).

For both users and websites, the user experience of safe single sign-on is essentially identical to social login—users can click a single button to register or login to a website or app without ever needing to create a new username or password. What makes it safe is:

1. Rather than logging in using a social network, a user is logging in from his/her own **personal private cloud**—a "cloud service" where the data is owned and managed entirely by the user, so the user's login activity and credentials remain private and not shared with anyone, not even the cloud service provider. "Cloud services" could be offered by news organizations or other service providers.
2. Rather than sharing data under the control and proprietary standards of a social network, users can share data directly under their own control, using open standards that will never lock them in to a single provider or service.
3. Rather than the login being subject to the terms of service and privacy policy of a social network (and its business interest in user data aggregation and monetization), safe single sign-on takes place under a trust framework designed to protect the privacy and data rights of both users and websites.
4. Rather than the security policies of a social network, which by definition must cater to the lowest common denominator, safe single sign-on can meet the security policies of websites and users. In particular, it can enable both sites and users to enjoy the benefits of multi-factor authentication without the need for websites to deploy new technology. The user can enroll once in multi-factor authentication for his/her private cloud (whether hosted locally or by a private cloud provider) and then use this strong authentication with any website that accepts safe single sign-on.

In short, safe single sign-on provides all the benefits of social login with none of the disadvantages.

One thing that makes safe single sign-on possible is the emergence of **private cloud networks**. A private cloud network enables private cloud owners—individuals, businesses, and application developers—to securely authenticate, send messages, and share data among their private clouds using a common protocol and trust framework. Each private cloud is owned and controlled entirely by the network member. The private cloud network includes a secure discovery service that enables members to authenticate, connect, and communicate among their clouds always under the full control and permission of each member.

AN EXAMPLE:

> Individual user Bill creates his own private cloud by registering to join a private cloud network in the way he would register to join an email network or a social network. The big difference is that with a private cloud network, Bill owns and controls all the information about him and he alone decides who to share it with when. Unlike an email network or a social network, the private cloud network provider does not have access to Bill's private cloud data and cannot monetize it or perform actions on Bill's behalf unless Bill's wants the provider to do so~~.~~ So Bill's private cloud is truly private and under his exclusive control.

Respect Network is the first company building a private cloud network based on the OASIS XDI semantic data interchange protocol and the Respect Trust Framework listed with the Open Identity Exchange.

Safe Single Sign-On for the ITE

From an ITE perspective, enabling users to have safe single sign-on via a private cloud network is a solution to lowering friction on all three dimensions involving end-users:

1. **For content access**, users registered with the ITE could have one-click access to controlled content from any ITE content provider. Users who are not registered with the ITE could sign up at any ITE content provider site in less than a minute.
2. **For user attribute exchange**, users could share (with as little as one click) attributes stored in their personal private cloud with any ITE member (individual or organization) to whom the user grants permission.
3. **For payment**, users can either use conventional payment mechanisms (such as an open account or subscription) securely stored in their private cloud or exchange a cryptocurrency (e.g., Bitcoin) or an ITE-sanctioned micropayment currency—again, with as little as one click. Periodic settlement services (i.e., user billing) can also be performed by members of the ITE network set up to do so.

Safe Single Sign-On Proof of Concept (POC) Proposal

Respect Network strongly supports the mission of the ITE and believes it is a perfect example of the type of ecosystem that can take maximum advantage of a private cloud network. To demonstrate this, Respect Network proposes to work with RJI and the other ITE POC participants to implement a safe single sign-on POC. This POC would include:

1. Providing personal private clouds to the set of ITE users participating in the POC.

2. Providing an XDI safe single sign-on button to the ITE content providers (real or mockup) participating in the POC.
3. Developing a simple XDI dictionary of user attributes to be shared in the ITE POC.
4. Developing the basic XDI link contracts for ITE safe single sign-on and attribute sharing.
5. Demonstrating how any ITE POC user can enjoy safe single sign-on and one-click user attribute exchange with any ITE POC content provider.

Optionally, the POC could also be extended to demonstrate user payment for content via one or more currency or microaccounting and aggregation options.