

Identidad Unificada en Internet

Juan Carlos Rodríguez Harika
Matricula: 55329

Universidad Católica Nuestra Señora de la Asunción

Abstract. Se habla del concepto de la identidad online, algunas de sus implicancias, y de las tecnologías y alternativas para una identidad unificada online.

1 Introduccion

Hace ya varios años, y cada vez más, Internet se ha vuelto una parte de nuestras vidas, con lo que viene un fenómeno que la mayoría de los usuarios experimentan, y este es, la identidad online.

Muchos de los sitios, servicios, aplicaciones en Internet, tiene administracion de identidad propia. Esto trae consigo como consecuencia, las multiples identidades online; un tema a ser tratado en el presente, junto con sus posibles soluciones, y las tecnologías asociadas a estas.

2 La Identidad Online

Con los servicios de comunicación e interaccion online (redes sociales, blogs, foros, wikis, etc), se hace necesaria la identidad online, que es la identidad social que el usuario establece en los sitios web y comunidades online.

La identidad online puede ser definida como “...el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital...” [1]

Aunque algunas personas prefieren utilizar sus nombres y datos reales online, otras personas optan por el anonimato, utilizando pseudonimos.

Así, cuando hablamos de identidad online, hablamos de lo que el usuario decide mostrar.

Según [2], en donde habla del concepto de *masking identity*; cuando un individuo interactua con una esfera social, este presenta una “mascara” de su identidad. Análogamente, un usuario al momento de construir su identidad online, tiene la libertad de elegir específicamente elementos de varios aspectos de su identidad.

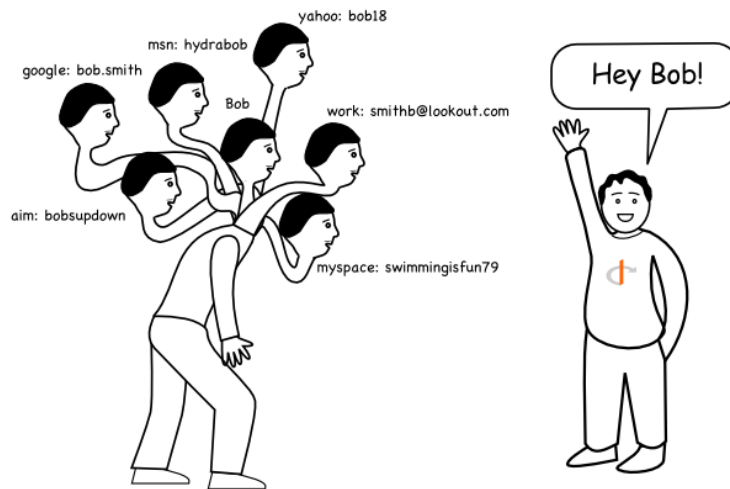
Así como la identidad online trata de lo que el usuario decide mostrar de si mismo, la *reputacion online* trata de los elementos que los otros usuarios otorgan

3 Identidades Online Multiples y Cuentas Multiples

El hecho de que muchos sitios, servicios y aplicaciones web, tengan administracion de identidad propia, nos lleva inevitablemente a tener varias identidades que mostrar, y en la mayoría de los casos, varias cuentas que administrar.

Tener varias identidades, tiene la desventaja del costo mental de personalizar y mantener cada una de estas identidades, y de tener que crear mas identidades a medida que se van usando mas servicios. El problema empeora, cuando con las multiples identidades, se tienen varias cuentas, todas con nombres de usuario y contraseas distintas, y con herramientas y reglas muy distintas para administrarlas. Esto puede significar menor seguridad (es muy comun que los usuarios utilicen la misma contraseña para todas sus cuentas, haciendo que la debilidad en la seguridad de una cuenta, comprometa todas las otras) y dar lugar a equívocos.

Sin embargo, hay gente que sostiene que la identidad de una persona, depende del contexto social, por lo que las multiples identidades, ademas permitir mayor personalizacion, tiene la ventaja de delimitar el contexto de los circulos sociales. Asi por ejemplo, si un usuario tiene una cuenta en un foro de juegos online, el emisor ya esta ubicado en el contexto, y la identidad que se muestra sera acorde, y distinta de, por ejemplo, la de un foro de software. Es por esto, que algunos creen, que en lugar buscar un ID unificado, seria mejor buscar una mejor manera de manejar nuestras multiples identidades.



4 Identidad Online Unificada y Single Sign-On

Contrariamente al fenomeno de las multiples cuentas, podriamos querer tener una sola instancia de autentificación, y utilizar estos credenciales con todos los servicios; este es el concepto de Single Sign-On.

Si quisieramos evitar tener multiples identidades, podriamos querer tener una sola identidad, esto es, un mismo conjunto de datos personales que se muestra de la misma manera para todos los servicios. Esto puede derivar directamente a partir de un sistema Single Sign-On. Pero una identidad unificada, no es tan definitivamente preferible como un Single Sign-On, asique podemos, para satisfacer ambas preferencias, tener un single Sign-On con la opcion de multiples identidades.

Para poder soportar la idea de un sistema de identificación unificada, se necesita de un Servicio Global de Administracion de Identidades (Global Identity Management System) [3].

OneName Corporation propuso, en [3], 7 requerimientos que debe de tener un servicio global de administracion de identidades:

1. **Portabilidad e Interoperabilidad** *Los dueños de la identidad deben de ser capaces de usarla contodas las aplicaciones, servicios, y dominios.*
2. **Extensibilidad** *Como no hay limite en los atributos que pueden estar asociados con una identidad, un segundo requerimiento clave es ofrecer un vocabulario de atributos extensible*
3. **Privacidad y Seguridad Negociadas** *Un servicio de administracion de identidades real, debe interoperar entre todas las jurisdicciones y dominios de confianza. In estas circunstancias, es imposible especificar toda la privacidad relevante y requerimientos de seguridad. Por eso, la privacidad y seguridad deben poder ser negociadas de un modo agente-a-agente*
4. **Responsabilidad** *Para que las personas y negocios alrededor del mundo puedan desarrollar confianza y confianza, en la habilidad de agentes automaticos de representar su identidad, la infraestructura de un servicio de administracion de identidad debe proveer responsabilidad adecuada, de la misma forma que bancos internacionales y sistemas de tarjeta de credito lo hacen hoy en dia*
5. **Autoridad de Registro Distribuida** *Por su naturaleza inter-jurisdiccional, un servicio de manejo de identidad no deberia depender de una sola autoridad de registro, sino proveer un protocolo y marco comun para cualquier numero de autoridades de registro*
6. **Autoridad de Certificación Distribuida** *Como con el registro, la naturaleza inter-jurisdiccional de un sistema de manejo de identidad, significa que no puede depereder en una sola red de confianza, sino que debe ofrecer un protocolo y marco extensible para muchas redes de confianza*
7. **Autoridad Governante Independiente** *Cualquier servicio global de manejo de identificaciones que cumpla con los requerimientos anteriores, requiere de un cuerpo governante que represente a todas las personas, negocios, organizaciones no gubernamentales y gubernamentales, equitativamente y sin discriminación*

5 Tecnologías

5.1 OpenID

OpenID es un standard abierto que describe como los usuarios pueden autenticarse de una manera descentralizada.

Los usuarios pueden crear cuentas con su proveedor de identidad OpenID preferido, y luego usar esas cuentas como base para autenticarse en cualquier sitio que acepte autenticación OpenID.

El protocolo OpenID no depende de una autoridad central para autenticar a un usuario; cada usuario puede elegir su proveedor de id.

Existen 3 partes que interactuan:

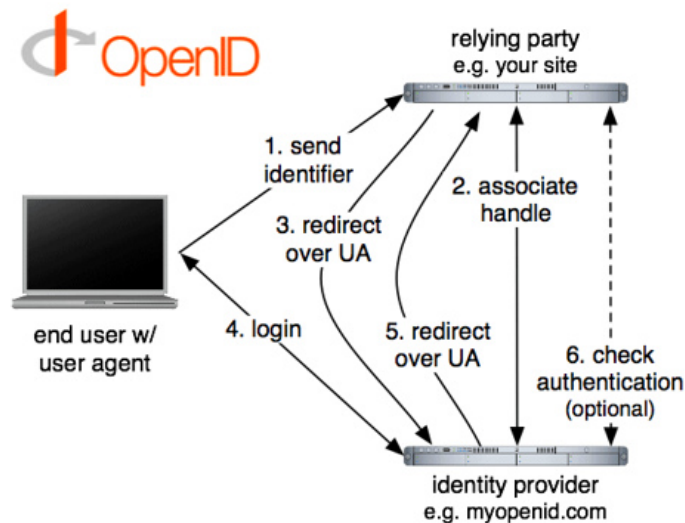
- **usuario-final** a quien la identificacion se refiere
- **relying party(RP)** es la pagina web o aplicacion que quiere verificar la identidad del usuario final. A estos tambien se les llama proveedores de servicios

- **OpenID provider** es el servicio que se encarga de registrar, administrar e identificar a los usuarios finales, cuando los proveedores de servicios (relying parties) lo requieran

El usuario final se registra con el OpenID provider de su preferencia, junto con cualquier información relevante. El usuario tendrá una URL o XRI, que identifique al OpenID provider, y opcionalmente al usuario final.

Al momento de identificarse, se siguen los siguientes pasos:

1. El usuario final accede al sitio del relying party, y si este lo admite, introduce su OpenID.
2. El usuario final es llevado al sitio del OpenID. Aquí el usuario final se autentica, y se verifica que el usuario realmente quiere identificarse en el Relying Party, y que información quiere que le sea proveída.
3. El usuario final es devuelto al sitio del Relying Party, con sus credenciales (que posteriormente el relying party verificará si son auténticas), y será identificado. En caso de haber rechazado la conformidad de que se le provea su identidad al relying party, el relying party será notificado de esto



Pros

- Código Abierto
- Múltiples proveedores (Yahoo, AOL, Google, ...)
- No hay proveedor central de datos de usuarios

Cons

- Solo se encarga de la Autenticacion (aunque puede ser combinado con otras tecnologias)
- La mayoría de los usuarios no-tecnicos no saben de su existencia, o no lo entienden.

5.2 OAuth

OAuth es un standard abierto que sirve para compartir recursos privados de un usuario (llamado en terminologia de OAuth el dueño del recurso), almacenados en un sitio (el servidor) con otro sitio (el cliente o consumidor).

Funciona de la siguiente manera:

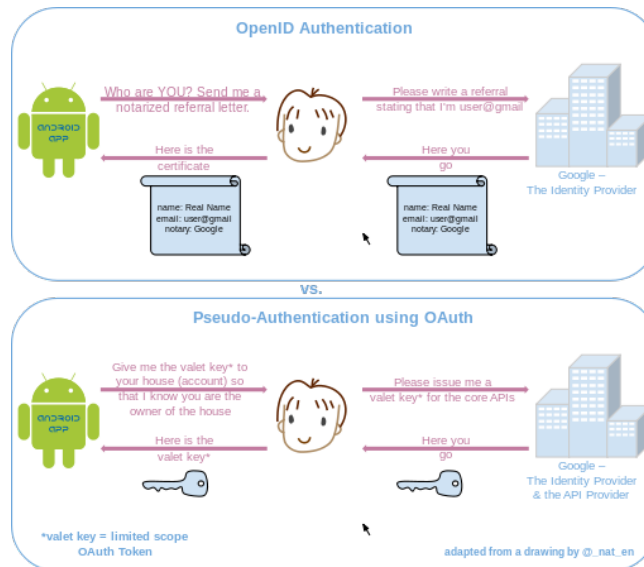
1. El dueño del recurso visita el sitio del cliente y este, al necesitar datos privados del servidor, lleva al usuario al sitio del servidor.
2. En el sitio del servidor, el dueño del recurso se autentica, y recibe un valet key. El valet key es un credencial destinado al cliente, limitado en acceso y tiempo. Es usando este credencial, que el cliente accede a la informacion privada del dueño del recurso.
3. El dueño del recurso regresa al sitio del cliente, y le provee del valet, key, que el cliente usará para acceder a los recursos.

OAuth no es un mecanismo para identificacion y autenticación (como por ejemplo lo es OpenID), sino que mas bien un complemento. No obstante, puede ser usado como metodo de autenticación, y varias tecnologias citadas aqui lo utilizan como base. El siguiente grafico describe con una analogia, las similitudes y diferencias entre la autenticacion con OpenID y OAuth. En ambos casos, el acceso al proveedor de identidad implicara autenticacion, a no ser que ya haya una sesion iniciada. En el caso de OpenID, la aplicacion autoriza el acceso por que el usuario tiene una carta de referencia autentica, de un proveedor de OpenID en quien confia. En el caso de OAuth, porque el usuario provee una valet key valida.

5.3 Facebook Login

Facebook Connect es una serie de APIs de Facebook que permite a usuario de facebook logearse en sitios, aplicaciones, etc. utilizando su identidad de Facebook. Mientas tenga la sesion iniciada, los usuarios pueden conectarse con amigos a travez de estos medio y publicar informacion y actualizaciones a su perfil de Facebook.

Facebook Login esta basado en OAuth. Cuando el usuario hace Login, la aplicacion tiene acceso a la informacion basica del usuario. Para obtener mas informacion o realizar otras acciones (como publicar en el perfil), necesita pedir permisos adicionales.



5.4 Google Friend Connect

Google Friend Connect usa standards abiertos tales como OpenID, OAuth y OpenSocial.

La API de Google Friend Connect provee las siguientes features:

- Integracion de características a través de HTML u otros lenguajes de marcado
- Personalizado de la apariencia de Google Friend Connect para que concuerde con los estilos y diseño del sitio
- Anuncios y contenido web que están asociados a perfiles individuales de los usuarios
- Integracion con sitios y servicios de terceros
- Integracion de Google Friend Connect con usuarios registrados y contenido del sitio

Varios gadgets sociales son usados para permitir la interacción con Friend Connect. Estos incluyen, entre otros, barras sociales, comentarios, ratings y opiniones, recomendaciones, eventos y juegos.

Love Da' Guacamole

Guac of the day

This recipe calls for preparing the guacamole in a molcajete, a mortar and pestle carved from volcanic rock. One of the world's oldest kitchen tools, it was used by the Aztecs in Mexico for grinding corn into flour.

Ingredients:
 1 ripe tomato, finely chopped
 2 Tbs. finely minced white onion
 2 serrano chillies, finely chopped
 1 Tbs. fresh lime juice
 1/2 tsp. sea salt, plus more as needed
 2 large avocados, preferably Haas
 2 Tbs. finely minced fresh cilantro

For the garnish:
 1 Tbs. small fresh cilantro leaves (optional)
 1 Tbs. finely chopped white onion (optional)
 1 Tbs. finely chopped ripe tomato (optional)

Directions:
 Put the tomato, onion, chillies, lime juice and the 1/2 tsp. salt in a molcajete or small bowl, and smash with a pestle or fork to a coarse paste. Cut the avocados in half, remove the pits and scoop the flesh into the tomato mixture. Add

Hi mussie [Settings](#) | [Sign out](#)

Your friends who are members:
[Annie](#) [Courtney](#) [Daniel](#) [David](#)

Members of guac5:
[Invite your friends!](#)

★★★★★ 1 posts

Rating: - add your review here -

★★★★★ This is the best guac EVAR
 mussie 5/8 8:35pm

(1 total)

Fig. 1. Friend Connect gadget example

6 Conclusión

La identidad unificada, es una opción interesante, tanto desde el punto de vista del usuario que navega, como del que genera contenido web, ya que facilita la interacción social online.

References

1. INTECO (Instituto Nacional de Tecnologías de la Comunicación, España): identidad digital y reputación online.
2. Cambridge University Press: Building Virtual Communities.
3. OneName Corporation: Requirements for a Global Identity Management Service.
4. Website, 24 September 2012
<http://en.wikipedia.org/wiki/OpenID>
5. Website, 24 September 2012
http://en.wikipedia.org/wiki/Facebook_Platform
6. Website, 23 October 2012
http://www.science20.com/daytime_astronomer/multiple_online_identities
7. Website 24 September 2012
en.wikipedia.org/wiki/OAuth
8. Website 24 September 2012
<http://hueniverse.com/oauth>