OpenBadges

Borrador - 18 de noviembre de 2014
jcea@jcea.es

Introducción

OpenBadges es un estándar propuesto por Mozilla[1] para crear un ecosistema de emisión, publicación y verificación segura de insignias. En la actualidad se está desarrollando dentro de la Badge Alliance[2].

Las insignias son ficheros gráficos[3] otorgadas por organizaciones para certificar el cumplimiento de un condición dada y publicitada (completar un curso, ser ponente en un congreso, superar cierto nivel en un videojuego). El receptor de una insignia puede mostrarla, a su discreción, como cualquier otro fichero gráfico: en su página web o blog personal, en su cuenta de LinkedIn, etc. Como gráfico que es se puede almacenar en el disco duro y enviar por correo electrónico como fichero adjunto.

Pero al contrario de una insignia normal, los OpenBadges contienen metainformación que permite verificar la identidad del individuo y la validez del logro conseguido. Posibilita, por ejemplo, que un entrevistador pueda comprobar la veracidad de las certificaciones presentadas por un candidato. En un mundo online global y conectado, esta característica resulta muy deseable. Dado que Internet no conoce fronteras, un verificador español podría comprobar la legitimidad de una insignia emitida por cualquier entidad mundial, y a la inversa.

Metainformación contenida en un OpenBadge

Una insignia OpenBadge contiene metainformación que permite verificarla. Consta de tres declaraciones:

1. La identidad de la organización que emite la certificación. Sus detalles y su URL.

   Ejemplo: *Asociación Python España.*

2. Los detalles generales de la certificación emitida. Una entidad puede emitir diversas certificaciones independientes. Típicamente se incluye una URL en la que se pueden leer los detalles concretos de la certificación, circunstancias que deben cumplirse para obtenerla, el diseño gráfico concreto que se utiliza, etc.

   Ejemplo: *Ponente de una charla de 45 minutos o más en PyConES 2014.*

3. Los detalles personales de la certificación. Es decir, la identidad del receptor de la misma, fecha de creación de la insignia, fecha de expiración si existe y -si está disponible- una URL conteniendo la prueba del logro que motiva la obtención de la insignia. Por ejemplo, si la insignia acredita la presentación de una ponencia en un congreso determinado, la URL podría apuntar al calendario del congreso o a las diapositivas utilizadas.

   Ejemplo: *Jesús Cea Avión, email: jcea@jcea.es, fecha: 9 de noviembre de 2014, URL: http://2014.es.pycon.org/talks* (idealmente debería apuntar a las diapositivas, cuando se publiquen).

1 http://openbadges.org/
2 http://www.badgealliance.org/
3 Los formatos soportados son PNG y SVG.

Verificación de OpenBadges

Las insignias son ficheros gráficos que, en general, no identifican visualmente al beneficiario. Los metadatos que le dan validez están encapsulados dentro del fichero gráfico y, en principio, requieren herramientas especializadas para acceder y mostrar las declaraciones.

La verificación segura de las declaraciones depende del tipo de OpenBadge generado:

- OpenBadges hospedados:

  Las tres declaraciones contienen tres URLs que apuntan a documentos idénticos en el servidor de la organización expendedora. Si el acceso se realiza de forma segura (HTTPS) el verificador puede confirmar que las tres declaraciones contenidas en la insignia coinciden exactamente con las tres versiones hospedadas en el servidor. Es decir, la insignia no ha sido manipulada. Dado que una de las declaraciones declara el receptor de la insignia, podemos confirmar también que no se ha producido una usurpación de identidad.

- OpenBadges con firma digital:

  Las declaraciones contienen una firma digital y la URL de la clave pública para verificarla. Si la URL indicada es un acceso seguro (HTTPS) y pertenece a una entidad emisora en la que confiamos, podemos verificar la firma digital sin necesidad de hospedar datos particulares de cada OpenBadge emitido.

Revocación de OpenBadges

Puntualmente puede ser necesario revocar un OpenBadge, por diversos motivos. Naturalmente no es posible alterar retroactivamente el fichero gráfico generado, en poder del destinatario. Las dos opciones son:

- OpenBadges hospedados:

  A la hora de acceder a la declaración que identifica la persona receptora, en vez de devolver el documento correspondiente el servidor devuelve un código de error 410 (“Gone”) y un texto explicativo del motivo por el que el OpenBadge ha sido revocado.

- OpenBadges con firma digital:

  Además de la URL de la clave pública que debe usarse para verificar las declaraciones del OpenBadge los metadatos incluyen también la URL de un fichero que contiene el listado de las revocaciones (y sus causas) emitidas hasta el momento. Esa URL debería ser segura (HTTPS).

  Cuando se realiza la verificación debe comprobarse que la declaración de usuario que estamos validando no aparezca en la lista de revocaciones.

Hospedaje de OpenBadges

Los OpenBadges son ficheros gráficos que se pueden almacenar y servir en Internet como cualquier otro fichero gráfico. En caso de disponer de una página web o un blog personal, la insignia puede hacerse pública como cualquier otro gráfico que sirva la web.

Opcionalmente existen servicios de *backpack*[4] para recopilar los OpenBadges de una persona (previa verificación), organizarlos por grupos y compartirlos de forma selectiva. De esta forma un individuo puede compartir sus OpenBadges de forma selectiva sin necesidad de disponer de recursos online propios.

4 Entre otros: http://backpack.openbadges.org/

Riesgo de fraude con OpenBadges

Una persona puede copiar el OpenBadge de un tercero o crear uno nuevo de forma maliciosa, pero no pasará la verificación de integridad (las declaraciones del OpenBadge no están en el servidor o la firma digital que las protege es inválida) o identidad (el OpenBadge es correcto pero la identidad del individuo no coincide).

Por lo tanto las insignias solo pueden ser falsificadas implicando a la entidad emisora.

- OpenBadges hospedados:

  Dado que la verificación requiere el acceso al servidor de la entidad emisora, este requiere almacenar información que puede usarse para auditar las insignias emitidas.

  Es decir, el servidor almacena las declaraciones de usuario de los OpenBadges emitidos. Si un usuario obtiene un OpenBadge ilegítimo no refrendado por el servidor, este no pasará la verificación de una tercera parte.

  La introducción de un OpenBadge falso en el servidor puede gestionarse a través de los mecanismos de control de acceso y auditoría de la entidad emisora.

- OpenBadges con firma digital:

  El estándar OpenBadges actual solo permite una única firma digital protegiendo y autentificando las declaraciones contenidas en los metadatos. La clave pública se almacena en el servidor, a disposición de cualquier parte interesada. La clave privada debe protegerse.

  Cualquier persona con acceso a la clave privada puede generar un firma digital válida y, por tanto, puede generar OpenBadges arbitrarios. Es más, dado que el servidor no guarda un registro de los OpenBadges emitidos no es posible detectar el uso fraudulento de la clave.

  En caso de filtración de la clave privada la entidad emisora puede revocarla simplemente eliminando la clave pública del servidor. Las verificaciones futuras fallarán debido a que el verificador no puede descargar la clave pública. Esto invalida todos los OpenBadges firmados con dicha clave, pasados y futuros.

  Si el estándar OpenBadges permitiese declarar varias claves públicas y exigiese una firma válida por cada una se podría disponer de cierto control. Pero no es el caso ahora mismo.

  Una opción a valorar es *thresholding cryptography*.

Thresholding cryptography[5]

Una posibilidad de afrontar los problemas anteriores sería emplear mecanismos de *thresholding cryptography*. Se trata de técnicas conocidas y documentadas, aunque no son de uso común. Si uno de los *shares* reside en un servidor es trivial, por ejemplo, llevar un registro de los OpenBadges generados, porque para crear la firma digital es imprescindible involucrar al servidor.

La destrucción periódica del *share* del servidor y la generación de una clave criptográfica nueva (mediante *thresholding cryptography*) permite expirar las claves sin afectar a los OpenBadges ya generados (siguen siendo válidos, su clave pública sigue estando disponible para la verificación aunque la clave privada se haya destruido) pero impidiendo generar OpenBadges nuevos con la clave compartida caducada.

5 https://en.wikipedia.org/wiki/Threshold_cryptosystem