# Autenticación delegada utilizando un perfil SSO de navegador web SAML (v2)

Por George B. Dobbs



*Para comentar sobre este artículo, visite nuestro repositorio de GitHub y envíe su problema.*

## Tabla de contenido

## Resumen

Este artículo se basa en una arquitectura de referencia de Administración de Identidades y Accesos (IAM, por sus siglas en inglés) genérica utilizada para describir un caso de uso común de un servicio de autenticación que utiliza el Lenguaje de Marcado para Afirmaciones de Seguridad (SAML, por sus siglas en inglés). Mostramos cómo un servicio (el tercero fiable o RP, por sus siglas en inglés) usa la capacidad de autenticación de un proveedor de identidad durante una acción de inicio de sesión único (SSO, por sus siglas en inglés) basada en la web.

## Introducción

Este artículo forma parte de un conjunto de artículos que ilustran varios componentes abstractos definidos en el artículo del Cuerpo de Conocimiento de IDPro, "Arquitectura de referencia de IAM".[1] Este artículo en particular se enfoca en un método específico de inicio de sesión único basado en la web a través del caso de uso común de un servicio (el tercero fiable) que usa la capacidad de autenticación de un proveedor de identidad (IDP, por sus siglas en inglés) a través del estándar Lenguaje de Marcado para Afirmaciones de Seguridad (SAML). Este método permite que el RP delegue la función de autenticación al IDP.

Este caso de uso generalizado se basa en la confianza entre el IDP y los terceros confiables (RP). Hay varias formas de hacer esto, este artículo asume que la confianza se basa en el uso de criptografía de clave pública, lo que implica el intercambio de certificados.

La especificación SAML define tres tipos diferentes de declaraciones de afirmación; este artículo es únicamente sobre la afirmación de autenticación.

La especificación SAML admite el mapeo de identidades entre diferentes nombres, lo que se conoce como identidad federada. Este artículo está restringido a un solo dominio, como ser una organización que brinda acceso a sus empleados a servicios basados en la web proporcionados por proveedores externos. En otras palabras, un único dominio de administración permite compartir los identificadores de los usuarios.

Incluso una revisión superficial de los documentos de estándares OASIS SAML revelará una estructura extremadamente rica y flexible. [2] Este artículo representa una porción muy pequeña de todas sus posibilidades, centrándose en el aspecto de tiempo de ejecución de la autenticación mediante el protocolo de mensajería web (HTTPS, por sus siglas en inglés).

---

[1] Dobbs, George, “IAM Reference Architecture,” IDPro Body of Knowledge, 30 September 2021, https://bok.idpro.org/article/id/76/.

[2] “OASIS SAML Wiki – Front Page,” wiki page, OASIS, https://wiki.oasis-open.org/security/FrontPage#SAML_V2.0_Standard (accessed 28 November 2022).

Técnicamente, estamos discutiendo lo que OASIS llama el perfil SSO del navegador web, utilizando el mecanismo POST. [3]

Esta sinopsis destaca la importancia de la Raíz de Confianza (*Trust Root*). La mensajería entre el IDP y el RP pasa a través del Agente de Usuario. El Agente de Usuario debe considerarse no confiable, ya que un agente corrupto podría modificar los mensajes. Para protegerse contra esta modificación, los mensajes están protegidos por una firma digital que debe ser validada. Es la autoridad de certificación común la que actúa como raíz de confianza para admitir estas firmas.

El tema de las firmas se puede complejizar rápidamente, por lo que no se trata en detalle aquí. La especificación SAML se basa en la sintaxis y el procesamiento de firmas XML de la recomendación W3C, que puede ser de interés. [4]

# Terminología

Consulte también la terminología en el artículo Cuerpo de Conocimiento de IDPro, "Arquitectura de referencia de IAM".

| Ítem | Definición |
|---|---|
| Agente de Usuario | Un Agente de Usuario es cualquier software que recupera, presenta y facilita la interacción del usuario final con el contenido web. [5] |

# Caso de uso

## Resumen

El usuario web trabaja a través de un Agente de Usuario para acceder a los recursos en un RP. La solicitud de acceso da como resultado una redirección del usuario a un IDP como parte de una acción de autenticación. Este resultado de la autenticación es una afirmación de autenticación que consume el RP y se usa para establecer un contexto de seguridad para el usuario web. En efecto, el RP ha delegado la autenticación al IDP.

[3] Hughes, John, and Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, Eve Maler, eds. "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS, 15 March 2005, https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf (accessed 28 November 2022).

[4] Bartel, Mark, and John Boyer, Barb Fox, Brian LaMacchia, Ed Simon, "XML Signature Syntax and Processing Version 1.1," Section: Core Validation, World Wide Web Consortium, 11 April 2013, https://www.w3.org/TR/xmldsig-core/#sec-CoreValidation, (accessed 28 November 2022).

[5] "User Agent Accessibility Guidelines (UAAG) 2.0," W3C Working Group Note, https://www.w3.org/TR/UAAG20/#glossary (accessed 28 November 2022).

## Tipos de arquitectura

Los diferentes tipos de arquitectura se definen en el artículo "Introducción a la arquitectura IAM" del Cuerpo de Conocimiento de IDPro. El caso de uso de la autenticación basada en SAML se aplica específicamente a la arquitectura de los entornos en la nube. [6]

## Actores

El usuario es el único actor. El usuario actúa a través del Agente de Usuario (el navegador). Los otros participantes en el caso de uso son "actores" del sistema, que mostramos como componentes.

## Componentes

Los siguientes componentes se definen en el artículo “Arquitectura de referencia de IAM”. [7]

- Repositorio de Auditoría
- Autenticación/Afirmación (parte del IDP)
- Registro de Identidad
- Terceros fiables (RP)
- Raíz de confianza

Tome nota que los documentos SAML se refieren a los terceros confiables como proveedor de servicios.

## Asunciones

El usuario desea acceder a un recurso protegido y ha solicitado acceso a través de un navegador web, el Agente de Usuario.

El RP tiene un solo IDP. El RP puede admitir varios IDPs, por lo que en ese caso se necesitaría un método para determinar cuál usar.

## Condiciones previas

Debe haber una confianza establecida entre el RP y el IDP antes de que se pueda usar SAML para la autenticación. “El mecanismo principal es que la parte que confía y la que afirma, tengan una relación de confianza preexistente que generalmente se basa en una

[6] Cameron, Andrew, and Graham Williamson, “Introduction to IAM Architecture,” IDPro Body of Knowledge, 17 June 2020, https://bok.idpro.org/article/id/38/ (accessed 28 November 2022).
[7] “IAM Reference Architecture,” https://bok.idpro.org/article/id/76/.

Infraestructura de Clave Pública (PKI, por sus siglas en inglés). Si bien SAML no exige el uso de una PKI, se recomienda el mismo". [8]

El IDP y el RP utilizan los mismos identificadores de usuario. La especificación SAML establece formas de mapearlos, pero no trataremos este tema aquí.

## Postcondiciones

El usuario está conectado al sitio del RP.

## Recorrido básico de eventos

A continuación, se muestra el "camino ideal", sin errores. Véase también el diagrama de secuencia más adelante. Consulte "Rutas alternativas" para ver algunas variaciones.

1. El usuario selecciona la función de inicio de sesión en el sitio del RP. Esta selección puede ser automática cuando el usuario intenta acceder al recurso protegido.
2. El RP determina que el usuario no ha iniciado sesión.
3. El RP prepara un mensaje de solicitud de autenticación, que el RP puede firmar. Se entrega al Agente de Usuario como un formulario dirigido al IDP, que se conoce porque hay un único IDP configurado. El Agente de Usuario (automáticamente a través de un script del lado del cliente) envía la solicitud al IDP.
4. El IDP se asegura de que el certificado de firma del RP siga siendo válido comprobando la revocación.
5. El IDP valida la solicitud e interpreta su contenido. Se chequean la firma y algunos valores de campo (como emisor, *AuthnContextClassRef*, etc.).
6. El IDP interactúa con el Agente de Usuario para recopilar el identificador y las credenciales del usuario. Por ejemplo, este podría solicitar un nombre de usuario y una contraseña, pero podría ser otra cosa.
7. El IDP utiliza su Registro de Identidad para validar las credenciales.
8. El IDP prepara un mensaje de respuesta, que el IDP firma.
9. La respuesta se envía de vuelta al Agente de Usuario con instrucciones para usar un HTTP POST para reenviarlo al RP. (La URL de destino del RP normalmente la conoce el IDP a través de la configuración inicial).
10. El RP se asegura de que el certificado de firma del IDP siga siendo válido comprobando la revocación.
11. El RP valida la respuesta e interpreta su contenido. La firma **debe** ser verificada. El RP lo compara con las afirmaciones ya activas para evitar la reutilización y realiza otras comprobaciones. El RP luego determina si la autenticación fue exitosa.

[8] Ragouzis, Nick, and John Hughes, Rob Philpott, Eve Maler, Paul Madsen, Tom Scavo, "Security Assertion Markup Language (SAML) V2.0 Technical Overview - Committee Draft 02," OASIS, 25 March 2008, https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf (accessed 28 November 2022)

12. En el cuadro, no se muestran los registros de auditoría que se están escribiendo. Los diversos componentes deben escribir los mismos.

## Rutas alternativas

El paso 3 se puede reemplazar con una redirección HTTP. Esta formulación es una composición permitida del enlace POST y el enlace *Redirect*. [9]

También hay alternativas al método de publicación en el paso 3.[10]

En términos de SAML, esta es la variante iniciada por el proveedor de servicios. También existe una alternativa iniciada por el IDP.

Los mensajes pueden estar encriptados. Por ejemplo, en el paso 8, el IDP puede cifrar y en el paso 10, el RP necesitaría descifrar la respuesta.

No recomendado: algunas implementaciones han ignorado la firma de solicitudes y la verificación de firmas, posiblemente debido a problemas de rendimiento.

## Rutas de excepción

La falta de autenticación en el IDP no devuelve una aserción.

La falta de validación de la firma indica que no se debe respetar la afirmación.

En el estándar se describen varias condiciones de error, como la expiración del período de validez.

[9] Cantor, Scott, and Frederick Hirsch, John Kemp, Rob Philpott, Eve Maler, eds. "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS, 15 March 2005, https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf (accessed 28 November 2022).
[10] Ibid.

## Diagrama de Secuencia

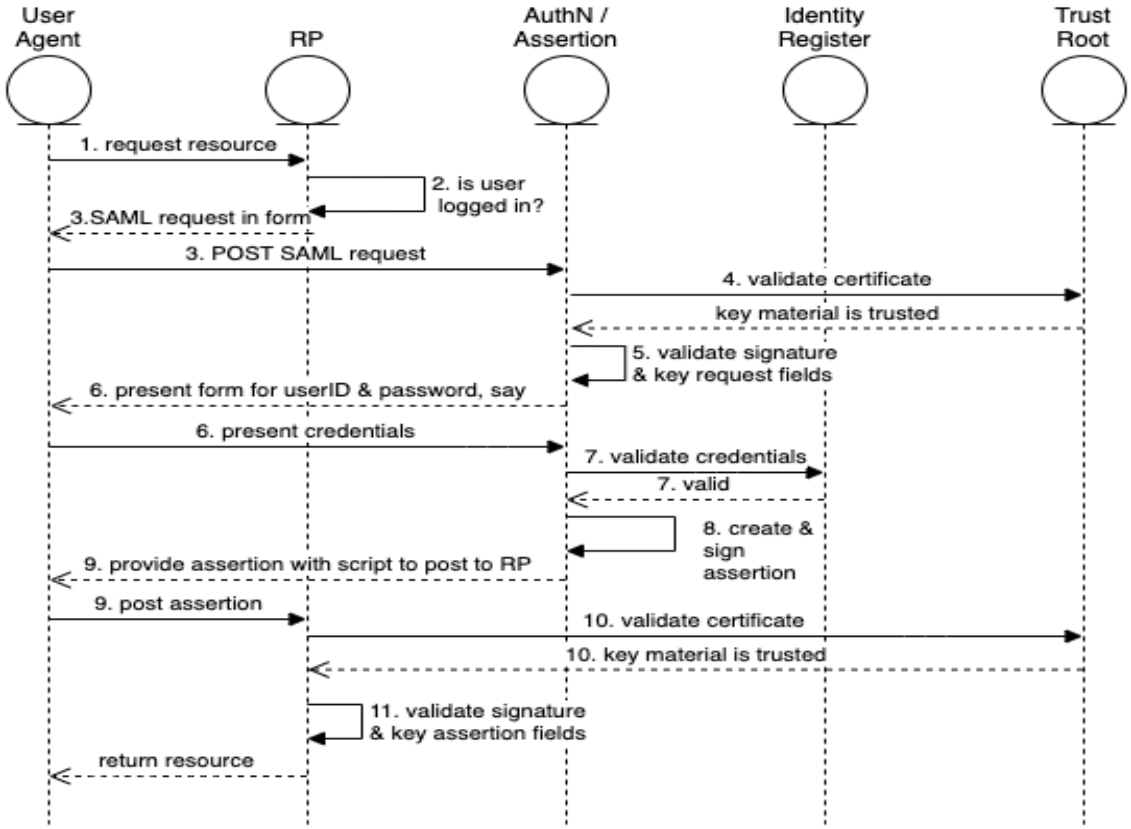


*Figura 1: El "camino feliz" del Perfil SSO del navegador web*

## Biografía del autor

George Dobbs dirige arquitectos en una importante compañía de seguros. También es el presidente del Comité del Cuerpo de Conocimiento de IDPro. Uno de sus intereses es modernizar el uso de las técnicas de Gestión de Identidad y Acceso que utiliza su compañía. Está particularmente interesado en el área de las aplicaciones orientadas al cliente, incluidos los enfoques para la prevención del fraude en centros de llamadas y contextos digitales. En relación con esto, está interesado en la evolución de la gestión de sesiones distribuidas, en particular, la terminación de sesiones distribuidas. Es miembro fundador de IDPro y representó a su empresa en el Grupo Directivo del Ecosistema de Identidad (IDESG). Antes de ocupar su puesto actual, dirigió el desarrollo de la identidad orientada al cliente para sitios web en otras tres aseguradoras. Ha dirigido un grupo local de usuarios de IAM desde 2004. Antes de eso, fue presidente del *Network Applications Consortium*.

## Agradecimientos

El autor quisiera expresar su gratitud a Chris Olsen y Bernard Carlier por su revisiones y sugerencias para mejorar este texto.

## Registro de cambios

| Fecha | Cambio |
|---|---|
| 2021-09-30 | V1 publicación |
| 2022-12-15 | V2 publicación; cambio de título, introducción y resumen de caso de uso aclarado; Ruta Alternativa incluye una sección de “no recomendado” |

## Referencias