Identificadores y Nombres de Usuario

Por Ian Glazer

Tabla de contenidos

Resumen

Un identificador es la forma que tiene un sistema de administración de identidades u otras entidades para referirse a una identidad digital. Sin embargo, el identificador utilizado por el sistema probablemente difiera del identificador utilizado directamente por el usuario y difiera definitivamente de los identificadores en otro dominio. El presente artículo repasa el concepto de identificadores en función de su relación con las personas, tanto desde la perspectiva del usuario como del sistema, así como su impacto en los sistemas que los utilizan.

Introducción

¿Qué son los identificadores y los nombres de usuario?

En el mundo físico usamos una variedad de formas para identificar a una persona o cosa. Desde números de serie o domicilios pasando por patentes de vehículos y seudónimos, a través de un identificador los humanos elegimos una opción específica dentro de un abanico de opciones similares. En el mundo digital, el comportamiento es el mismo. Los sistemas informáticos y las personas que trabajan en ellos escogen un identificador para diferenciarse dentro de una gama de opciones similares. En términos más formales, en el contexto de la administración de identidades podemos pensar en los identificadores como una forma que tienen los sistemas de administración de identidad para referirse a una identidad digital.

Es posible que la persona asociada a esa identidad digital no use el mismo identificador que utiliza el sistema. De hecho, lo más probable es que así sea. Típicamente, la persona utiliza un identificador amigable con el humano. Para poner las cosas en claro, llamaremos nombre de usuario a la forma que tiene una persona poseedora de una identidad digital para identificarse.

¿Por qué considerar los identificadores y los nombres de usuario?

La forma en la que los sistemas se refieren a las identidades digitales y la forma en la que las personas se refieren a sus identidades digitales en un sistema son de crucial importancia. Los identificadores y los nombres de usuario son uno de los componentes más utilizados en un sistema de administración de identidad digital. Repercuten en la usabilidad, seguridad, satisfacción del cliente y operaciones del sistema, y habilitan (o previenen) relaciones directas entre sistemas y la gestión de cuentas de usuario. Son aplicables en casos de uso de negocio a empleado (B2E, por sus siglas en inglés), negocio a negocio (B2B, por sus siglas en inglés), negocio a cliente (B2C, por sus siglas en inglés) y negocio a negocio a empleado (B2B2C, por sus siglas en inglés)

No tener en consideración los identificadores y especialmente los nombres de usuario puede tener impactos negativos directos en los proyectos y sistemas en los que estés trabajando.

Tipos de Identificadores

Los identificadores vienen en dos variedades: internos y externos. Los identificadores internos son la forma en la que un sistema se refiere a una identidad digital. Los formatos de los identificadores digitales pueden variar mucho entre sí. Uno de los formatos más comunes de identificadores internos es el identificador único universal (UUID, por sus siglas en inglés). Dentro del IETF RFC 4122, se especifican 4 variedades o versiones de UUIDs.[1] Muchos sistemas utilizan la versión 4 de UUID (a menudo referida como UUID4), que son identificadores generados aleatoriamente. Un ejemplo de UUD4 es: d5372288-697b-42bf-928a-562aca0deeaf.

Dicho esto, no todos los identificadores internos son UUIDs. Los sistemas pueden utilizar otras vías de identificación única de una cosa específica dentro de un abanico de opciones similares. Algunos ejemplos de esto incluyen identificadores que tienen un significado específico para el sistema pero que no lo tienen por fuera de él, como, por ejemplo: "005o0000000s4Hu."

El segundo tipo de identificadores son los identificadores externos. Un identificador externo es la manera en la que una persona poseedora de una identidad digital se refiere a dicha identidad cuando interactúa con un sistema. Estas incluyen, pero no se limitan a un número de teléfono, un correo electrónico, un seudónimo o un alias.

En algunos casos, un identificador de sistema puede utilizarse con fines internos y externos. Dado que los correos electrónicos deben ser únicos en una organización (por ej. una empresa) o en un dominio (por ej. universidades o médicos), la 'net id' del miembro como por ejemplo la primera parte de su correo electrónico, será utilizada dentro de sistemas corporativos como un identificador de usuario. Una 'net id' puede componerse de la primera inicial, la segunda inicial, el apellido y un número que garantice su singularidad.

Terminología

- Identificador interno: la forma en que un sistema de administración de identidades se refiere a una identidad digital.
- Identificador externo: la forma en la que una persona que controla una identidad digital se refiere a esa identidad cuando está interactuando con un sistema.
- Nombre de usuario: término común usado para referirse a un identificador externo.

[1] Leach, P., Mealling, M., y R. Salz, "*A Universally Unique IDentifier (UUID) URN Name*space", RFC 4122, DOI 10.17487/RFC4122, Julio de 2005, <https://www.rfc-editor.org/info/rfc4122>.

Aspectos de los nombres de usuario

Al momento de considerar qué formato deberían tener los nombres de usuario, un profesional de la identidad debería tener en cuenta los cinco principios rectores de los nombres de usuario. Como mínimo, el formato del nombre de usuario debe ser considerado por el profesional tanto en proyectos de nueva creación como cuando nuevos servicios B2C y B2B2C se están creando. A menudo, especialmente en escenarios B2B, los nombres de usuario tienen formatos ya establecidos en generaciones previas de sistemas adoptando una cualidad casi mítica. Sencillamente no es razonable cambiar los formatos de nombres de usuario. Demás está decir que un cambio de nombre de usuario no debe ser tomado a la ligera, especialmente en un escenario de empresa B2B.

Las aplicaciones en la nube son un área de potencial confusión en cuanto al nombre de usuario. En una aplicación de varios inquilinos (*multitenant application*), los nombres de usuario deberían ser comunes, por ej. el nombre de usuario para una identidad digital en una aplicación es el mismo que se usa en otra aplicación. Sin embargo, en algunos casos un usuario establece una cuenta en una aplicación SaaS y escoge otro nombre de usuario. Si esta aplicación se conecta posteriormente al entorno de administración de identidad, será necesario aplicar un mecanismo de transformación. Una opción son las API *gateway* o los servicios proveedores de identidad que almacenan varios nombres de usuario.

Los cinco principios rectores que los profesionales de la identidad deben considerar establecen que los nombres de usuario:

- No son secretos
- Deben ser clasificados como información pública
- Deben ser fáciles de recordar
- Deben ser únicos
- Deben ser recuperables

Secreto

Los Números de Seguridad Social (SSN, por sus siglas en inglés) de Estados Unidos son el ejemplo perfecto de lo que no se debe hacer con los nombres de usuario.[2]

Los SSN se crearon como un identificador interno. Originalmente los utilizaba la Administración de Seguridad Social para asociar a un humano a sus ganancias y eventualmente a los subsidios que percibía, como parte de sus procesos de negocio. Para ejecutar sus procesos de negocio, este identificador interno se compartía con personas y

[2] Carolyn Pucket, "The Story of the Social Security Number, Social Security Bulletin", Vol. 69, No 2, 2009, https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

empleados. Pero el uso de este identificador interno se expandió. Los negocios empezaron a usar los SSN como una forma de identificación de las personas ante un negocio. Es decir que esencialmente los negocios transformaron este identificador interno en un nombre de usuario. Este uso secundario se basaba en la idea de que solo las propias personas conocían su SSN y por lo tanto el mismo era secreto, asumiendo así que el portador del SSN era la persona correcta. Allí es donde las cosas empezaron a fallar.

La necesidad de este secreto específico se extendió a muchísimos procesos de negocio a lo largo de nuestra economía y amplificó masivamente los daños cuando los *brokers* de información padecieron infiltraciones.

La lección aprendida de los SSN es que los nombres de usuario no pueden ser secretos. Si compartes un identificador interno con terceras partes por fuera de tu organización, habrás transformado ese identificador interno en información pública y por lo tanto no podrá ser secreto.

Si tienes un nombre de usuario o un identificador interno que debe ser tratado como un secreto entonces lo que tienes en tus manos es un mecanismo de autenticación y no un nombre de usuario. Eso significa que debe tener un tratamiento similar al de una contraseña.

Un tema para profundizar en otra ocasión: en términos generales, los datos biométricos no deben ser secretos. Una persona no puede mantener en secreto sus huellas digitales, geometría facial o sus iris. Por esto, un sistema o proceso puede usar datos biométricos como identificadores externos, pero únicamente porque son justamente "solamente" identificadores. Para garantizar que la persona correcta es quien está presentando los datos biométricos es necesario tener algún nivel de autenticación. Este grado de incertidumbre explica por qué la prueba de vida y la verificación de actividad en vivo son cruciales. Por ejemplo, no se puede aceptar una huella digital sin verificar que el dedo es real, tiene sangre corriendo por sus venas y que no se trata de un dedo falso hecho de gelatina[3].

Público

Asegurarse de que los nombres de usuario no son secretos no es suficiente. Los profesionales de la identidad también deben clasificarlos como "públicos" en su esquema de clasificación de datos. Esta acción aplica a empleados, socios y clientes por igual.

[3] John Leyden, "*Gummi bears defeat finger print sensors*," The Register, 16 de mayo de 2002, https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/.

El hecho de clasificar los nombres de usuario como públicos no implica de ninguna manera que los atributos relacionados al individuo sean públicos. Por seguridad, es evidente que estos atributos no pueden ser usados en un nombre de usuario. Ten en cuenta un sistema de clasificación de datos de cuatro niveles simple:

- Público: esta información puede ser compartida libremente dentro de los límites de la organización, con un bajo nivel de preocupación.
- Restringidos: esta información es esencial para el proceso de negocio y no se compartirá por fuera de los límites de la organización. Solo los propietarios de los datos, empleados y contratistas pueden acceder a estos datos.
- Confidencial: esta información es crucial para las operaciones comerciales. Si estos datos traspasan los límites organizacionales puede ocurrir un daño significativo.
- Secreto: estos datos son extremadamente sensibles para la organización. Únicamente un pequeño y selecto grupo de personas y sistemas pueden accederlos.

En un mundo ideal, el número de fidelización (otro tipo de identificador) de una aerolínea u hotel está clasificado como “Restringido”. Los nombres de usuario deben clasificarse como “Público”. Los números de fidelización de una aerolínea u hotel evidencian el problema que implica un identificador “público” que contiene atributos que tienen un valor.

Además, clasificar los nombres de usuario como públicos refuerza la idea de que los identificadores no pueden ser secretos.

Se recomienda que los nombres de usuario se clasifiquen como información pública en un sistema de clasificación de datos, pero esto no significa de ninguna manera que los nombres de usuario deban ser divulgados (por ej. listados en un sitio web público) ya que eso sería un ataque de enumeración autoinfligido.

Fácil de recordar

“Moby Dick” de Herman Melville es una de las piezas canónicas de la literatura estadounidense y su primera frase es “Llámame Ishmael”. Ishmael (el nombre de usuario) no es la parte más importante de la frase sino “llámame”. El poder de nombrar algo es el poder de controlarlo. Y al llamarse Ishmael el individuo toma el control sobre sí mismo, distinguiéndose del lector y del autor.

Apoyando su autodeterminación, las personas se asignan nombres lo cual es crucial en el mundo digital. Los nombres de usuario deben ser autogenerados en escenarios B2C y B2B2C, es decir que la persona debe tener el poder de crear su nombre de usuario preferido. Considerar los nombres de usuario autogenerados es importante también en escenarios B2B y B2E.

Muchas empresas tienen un formato estándar de nombre de usuario y lo trasladan a casos de uso B2C y B2B. Un formato clásico de nombre de usuario se conforma de la primera inicial + el apellido. Por ejemplo, Sally Smith tendría el nombre de usuario “ssmith” y si el mismo no es único, un número aleatorio se le agregaría. Si bien es eficaz, este formato de nombre de usuario basado en los hábitos no satisface el deseo de la autodeterminación que es crucial en los casos de uso B2C.

Cuando los nombres de usuario no son fáciles de recordar implican proveer más asistencia técnica, más atención al cliente y un incremento en las llamadas de recuperación de cuenta. También alimentan los identificadores duplicados porque a menudo las personas olvidan el identificador que usaron para registrarse.

Al crear un esquema de nombre de usuario, se debe ofrecer opciones al usuario. Si se solicita un correo electrónico como nombre de usuario y en el siguiente paso el usuario dice “no me contacte por correo electrónico”, se genera un dilema significativo. Para ofrecer opciones al usuario, es importante contar con varios esquemas de nombre de usuario como el correo electrónico o un seudónimo creado por el usuario. Mantener varios esquemas añade un nivel de complejidad, pero empodera al usuario y genera autodeterminación y satisfacción del cliente.

Único

Los nombres de usuario deben ser únicos. Los identificadores internos deben ser únicos. Ninguna de estas declaraciones debería ser controversial, pero existen matices.

Decir que un nombre de usuario debe ser único no es suficiente, uno debe tener en cuenta el alcance de dicha singularidad. ¿Es acaso el nombre de usuario único:

- a nivel individual en el servicio?
- a nivel del inquilino (si tienes varios inquilinos)?
- dentro de un espacio de nombres de un servicio o conjunto de servicios?
- globalmente a lo largo de todos tus servicios?
- universalmente?

¿Hay una idea clara del alcance para el cual se está diseñando? Aún si la hay, esta puede cambiar; los profesionales deben considerar si a futuro habrá fusiones internas de sistemas o si soporta varias fusiones y posibles adquisiciones a largo plazo.

Asimismo, la singularidad tiene implicaciones que dependen del tipo de identificador. Los nombres de usuario y los identificadores internos no tienen el mismo alcance de singularidad. Por ejemplo, mientras que un identificador interno debe ser único

globalmente, un nombre de usuario puede ser único solamente en un subconjunto de sistemas de una empresa. Los identificadores internos deben ser únicos dentro del alcance del servicio, por ejemplo, únicos en un servicio específico de una empresa. Para mitigar potenciales re-identificaciones de sujetos de datos, estos identificadores deben ser únicos a nivel global. Por otra parte, una persona podría usar su correo electrónico para iniciar sesión en varios sistemas - se trataría de un nombre de usuario único a nivel de servicio.

Adicionalmente, no se debe hacer que el nombre de usuario y el identificador interno sean el mismo dentro del mismo sistema. Este fue uno de los errores cometidos con el Número de Seguridad Social en Estados Unidos. [4] Los profesionales deberían evitar esto aunque sea solo porque cambiarlos posteriormente es enormemente desafiante. Más aún, un esquema de nombre de usuario común es el correo electrónico y este puede cambiar a lo largo de la vida de una persona porque se casa o se divorcia, entre otros motivos. Realizar estos cambios en el nombre de usuario en un esquema donde el nombre de usuario y el identificador interno son el mismo, requiere que todos los sistemas que utilizan el "viejo" nombre de usuario/identificador interno deben ser notificados del cambio y actualizados. En un entorno complejo esta tarea puede resultar casi imposible.

Una última consideración para tener en cuenta es la reutilización de nombres de usuario. El servicio de correo electrónico de Yahoo! permite que las personas utilicen un correo electrónico que anteriormente perteneció a otra persona. Los números de teléfono son regularmente reutilizados. En este caso, el nombre de usuario puede seguir siendo único pero la persona que lo posee cambió. Esta transición es complicada ya que el nuevo propietario del correo electrónico o teléfono parece, en muchos casos, un atacante.

Recuperable

Los nombres de usuario deben ser recuperables, es decir que debe haber una manera para que la persona recupere su identidad digital. Recuperar significa volver a asociar a la persona a su identidad digital; esto no significa necesariamente que vayan a utilizar el mismo nombre de usuario nuevamente.

En ese sentido, la recuperación va más allá que recordarle a la persona qué correo electrónico usaba para iniciar sesión. Imagina decirle a una persona que el correo electrónico que usaba era el correo electrónico de su antiguo trabajo al cual ya no tiene acceso. Esto deja a la persona con pocos recursos: contactar al servicio de asistencia técnica o cambiarse a otro servicio.

[4] Pucket, vea Los usos expandidos de SSN, https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

La recuperación es una re-asociación y realizarla a salvo requiere a menudo volver a demostrar que el individuo es quien dice ser. Especialmente en escenarios B2C, este proceso de re-demostración requiere especial atención ya que tiene implicaciones significativas en la seguridad y en la satisfacción del cliente.

Conclusiones

Los identificadores son necesarios en un sistema de identidad y los identificadores internos y externos cumplen distintos propósitos. Si bien ambos identificadores pueden ser el mismo, esto debe ser considerado con mucha cautela por parte del profesional IAM. Los identificadores externos, también conocidos como nombres de usuario, deben tener en cuenta los siguientes cinco principios rectores:

- Los nombres de usuario no deben considerarse un secreto.
- Los nombres de usuario deben clasificarse como información pública.
- Los nombres de usuario deben ser fáciles de recordar.
- Los nombres de usuario deben ser únicos.
- Los nombres de usuario deben ser recuperables.

Cada uno de estos principios tiene implicaciones que el profesional de la identidad debe tener en cuenta a la hora de desarrollar un sistema de administración de la identidad. Crear una infraestructura de nombre de usuario forma parte de las tareas de orquestación de la identidad.