



Identidad digital: uno de los nuestros

Desde hace unos años se habla de los sistemas de Identity Management (IdMs) como aquellos sistemas que integran procesos de negocio, políticas de actuación y tecnologías para facilitar el control de las organizaciones sobre el acceso que tienen sus usuarios a aplicaciones y recursos críticos, como pueden ser datos personales o informaciones estratégicas.

Bajo este nombre se colocan aquellas tecnologías utilizadas para la **Gestión de Identidades** (provisión de cuentas, automatización de flujos, administración delegada, sincronización de contraseñas, etc.), para el **Control de Acceso** (basado en políticas, *Single Sign-On/Off*, *Web-SSO*, *Reduced-SSO*, etc.), para el establecimiento de **Servicios de Directorio** (Repositorios de identidades, replicación y sincronización de meta-datos, virtualización de directorios, etc.), y otras tecnologías como aquellas basadas en el **Control de Acceso basado en Roles** (RBAC) y la **Federación de Derechos de Acceso**. Dentro de este último punto podemos encontrar algunas iniciativas importantes como son el consorcio Liberty Alliance, la propuesta universitaria Shibboleth, la iniciativa de federación dentro del esquema de los Web Services y la solución Live ID de Microsoft.

En los sistemas basados en la Federación de Identidades lo que se hace es reconocer tres tipos de agentes no siempre bien diferenciados: por una parte tenemos aquellos que conocen parte de las identidades puestas en juego, o Identity Providers (los que saben de ti), enfrente están los que quieren conocer partes de la identidad invocada, o Identity Consumers (los que preguntan sobre ti) y, por último, el usuario final que es el titular de la identidad puesta en juego.

Una de las ventajas que suponen los sistemas basados en la federación de la identidad es que reducen considerablemente el número de agentes que realmente deben estar bien identificados a través de sistemas jerárquicos y poco flexibles como es el caso de las PKIs. Las soluciones federativas lo que intentan es soslayar el problema de escalabilidad que tienen sistemas de gestión de identidades basados en certificados o equivalentes: el número de consumidores individuales que hay en la Unión Europea es mucho mayor que el número de empresas o instituciones que organizan y constituyen su tejido

El problema de la Identidad Digital es tan antiguo como los sistemas operativos multiusuario y las redes, pero todavía sigue sin resolverse. Con la llegada de los intereses comerciales a Internet, el problema toma tintes más radicales ya que todo el mundo acepta que sin identidad y responsabilidad no es posible hacer negocios en Internet. Los sistemas clásicos -PKIs, PMIs y demás acrónimos incluidos-, no han sabido resolver el problema, por lo que aparece el concepto de Federación de Identidades que es la actual promesa para resolver el problema que parece frenar el comercio y la administración en Internet.

administrativo o económico. Si todas esas entidades fuesen las depositarias de las identidades parciales de todos los ciudadanos europeos, el tamaño de la jerarquía o jerarquías de clave pública que serían necesarias para resolver el problema de la identificación sería mucho menor.

El problema de la federación de identidades es que ésta supone la cesión parcial o total de la identidad, y eso puede ser tolerable o no dependiendo del escenario

Hay que definir si la tecnología debe principalmente favorecer y facilitar el intercambio de datos personales para agilizar los procesos o si, por el contrario, debe primar la defensa de la intimidad individual y defender el libre ejercicio de la identidad, ante intereses comerciales y de otra índole.

que consideremos. Si nos centramos en entornos laborales, la identidad que se debe federar es de carácter funcional y sólo tiene sentido dentro de los organigramas de las empresas o corporaciones; el tesorero que autoriza un pago lo hace en concepto de tal, y no como persona individual que puede ser despedida dos días después y no por ello va a sufrir la función y concepto de tesorería.

Otra situación distinta es cuando los usuarios cuya identidad se pretende federar son personal, clientes, individuos particulares. En este caso, la protección de la intimidad de éstos debe estar por encima de cualesquiera intereses o prácticas comerciales. Además de esto, no hay que olvidar que, en justa medida, la cesión de identidad debería ir acompañada de la cesión de las responsabilidades asociadas con ella; dicho de otro modo, si un sistema puede llegar a representarme completamente en una transacción, es ese sistema el que asume las responsabilidades de ella y no el titular legítimo de la identidad federada. Si para evitar este sinsentido, lo que se hace es poner cláusulas que impiden esta transferencia, en ese caso, la indefensión del individuo es total y atenta contra uno de

los derechos fundamentales que es el derecho a una identidad propia y exclusiva, sobre la que ejercitar derechos y asumir responsabilidades. La cesión del ejercicio de la identidad manteniendo la responsabilidad de ello es como vender el alma, pero no al Diablo, sino a entidades e intereses comerciales con mucho menos *glamour* que éste, pero que pueden amargarle mucho a uno la vida.

Puede que los sistemas basados en la federación de identidades puedan llegar a tener éxito dentro de entornos empresariales y administrativos ya que, en esos casos, la identidad que se reparte es de claro carácter funcional, está plasmada en el correspondiente organigrama y, además, todas ellas emanan de la misma entidad jurídica o institución de que se trate. En el caso de las identidades individuales la cesión total o parcial de la identidad torpedea el principio de responsabilidad y eso hace que las tecnologías federativas propuestas, y las que puedan llegar a aparecer en el futuro, podrán ser útiles en transacciones empresa a empresa (B2B) pero deberían ser desterradas de las relaciones (B2C) con usuarios humanos finales en cualquiera de sus aspectos: como ciudadano, como cliente, como paciente, etc.

Todas las iniciativas que están encima de la mesa (Liberty Alliance, Shibboleth, WS-IF y Live ID) se encuentran actualmente en avanzado estado de desarrollo pero, en todas ellas, el problema de cómo resolver las disputas que se plantearían cuando las cosas van mal –y eso siempre

termina por ocurrir–, es un tema que ninguna de ellas tiene realmente planteado y, menos aún, resuelto. Ya sólo por este motivo podemos decir que estas tecnologías no están maduras, y que todavía les queda mucho trecho por recorrer antes de poder ser una alternativa seria para llenar la vacante actual de lo que entendemos como Identidad Digital en el sentido más amplio posible.

Modelos tecnológicos precisados

Además de la resolución de disputas, otro tema que está pendiente es decidir qué modelo de tecnología se quiere o se necesita. Las tecnologías no son inocuas, por lo que siempre hemos de tener en cuenta que una tecnología siempre favorece más a unos promotores que a otros (caso Liberty versus Live ID/Passport, por ejemplo); también hay que definir si la tecnología debe principalmente favorecer y facilitar el intercambio de datos personales para agilizar los procesos o si, por el contrario, la tecnología debe primar la defensa de la intimidad individual y defender el libre ejercicio de la identidad, ante intereses comerciales y de otra índole.

Sin dar una respuesta clara de cómo se resuelven todos y cada uno de los posibles conflictos y sin definir claramente quién se beneficia mayoritariamente de la adopción de una u otra tecnología, el desembarco real y universal de estas soluciones, en lo que hoy conocemos como Internet, es algo que se va a demorar largamente. Algunos incluso creen que no va a haber respuesta satisfactoria al primero de los retos por el riesgo que supone gestionar la identidad de otros y asumir con ello la correspondiente cuota de responsabilidad; respecto al segundo reto, puede decirse que no va a ser fácil conciliar los intereses reales de individuos y corporaciones, por lo que estaríamos ante un tipo de tecnologías que no darían la talla en cuanto a ser solución al problema planteado, que no es otro que el de la Identidad Digital con mayúsculas. ■

JORGE DÁVILA MUÑOZ

Consultor independiente
Director

Laboratorio de Criptografía
**LSIIS – Facultad
de Informática – UPM**
jdavila@fi.upm.es