Autenticación Adaptativa de Safelayer: seguridad aumentada mediante información contextual

En la actualidad, la credencial más usada sigue siendo la contraseña de usuario, aunque cada vez está más aceptado que proporciona una seguridad insuficiente para la mayoría de aplicaciones. La actividad digital en la web atrae a empresas, consumidores y ciudadanos, con crecimientos exponenciales impulsados por la troika que forman el cloud computing, la movilidad y las redes sociales. Pero, a la vez, las amenazas y los ataques también crecen, encabezados por los de phishing, pharming y suplantación en general. En este entorno, una solución tecnológica que permita escalar la seguridad partiendo de credenciales populares, aunque poco seguras, de forma dinámica hacia credenciales de alta seguridad en función del riesgo y simplificando al máximo la experiencia del usuario puede resultar muy adecuada.

Contexto, riesgo y factores de autenticación adaptativa

La autenticación tradicional se basa en una única credencial que aglutina uno o varios factores. Con un mínimo de dos factores se pueden obtener niveles altos o muy altos de seguridad, mientras que con un único factor se obtienen niveles medios o bajos. Por ejemplo, las credenciales basadas en contraseña de usuario contemplan un solo factor del tipo “algo que se sabe”, mientras que las credenciales PKI almacenadas en tarjeta contemplan dos factores: “algo que se tiene” (el certificado en dispositivo seguro) y “algo que se sabe” (el PIN para poder usarlo). En esta línea, en general, se establece la siguiente relación: a mayor seguridad, menor usabilidad y mayor coste total.

Una estrategia de autenticación más moderna se basa en establecer diferentes capas de seguridad a lo largo de la interacción del usuario con el sistema, requiriendo diferentes factores de autenticación adicionales a medida que se requieran. Por ejemplo, un usuario se autentica en una aplicación web con una contraseña (“algo que sabe”) y sólo se le solicita que introduzca un código que recibe por SMS en su móvil (“algo que tiene”) cuando debe realizar un acceso sensible. Esta estrategia se puede reforzar con factores adicionales tales como la biometría del comportamiento (“algo que se es”) e información de contexto del usuario (“algo que se hace”), consiguiendo mayores niveles de seguridad a la vez que se mantiene la facilidad de uso.

La combinación de múltiples factores, entre ellos la observación del contexto del usuario, contribuye a detectar y mitigar posibles riesgos. Por ejemplo: se detectan accesos desde dispositivos no habitual es para el usuario, diferencias geográficas imposibles entre dos accesos consecutivos, o patrones de tecleo que difieren del patrón del usuario, lo que puede indicar un uso fraudulento del dispositivo o un ataque automatizado. En tal caso, el sistema de **autenticación adaptativa** responde a esta situación anómala que apunta **riesgo de suplantación** elevando la exigencia de seguridad y solicitando un nuevo factor de autenticación al usuario, que éste deberá presentar con éxito para conseguir el acceso. A este proceso adaptativo también se le suele denominar autenticación basada en riesgo o contextual.

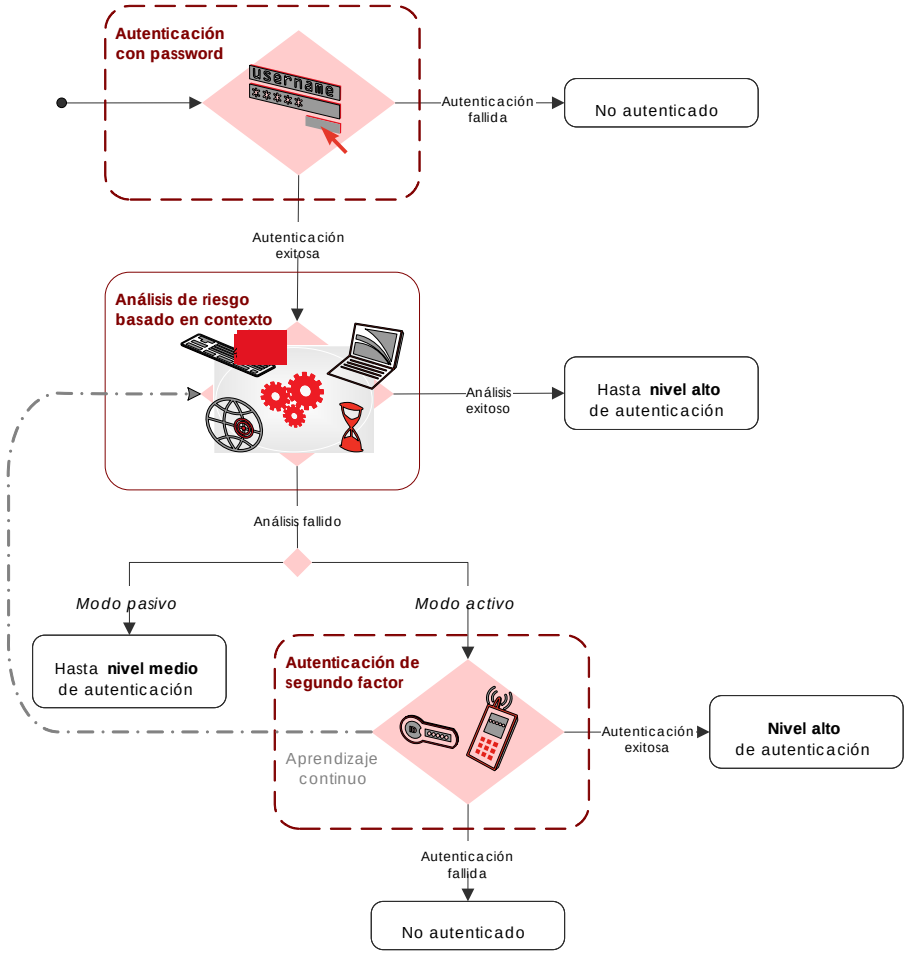
Aumentando la seguridad, maximizando la usabilidad y minimizando coste de la autenticación

Basado en la combinación de factores, el contexto y un análisis de riesgo, TrustedX Autenticación Adaptativa de Safelayer ofrece las siguientes características y propiedades clave:

- **Primera línea de autenticación configurable**, que se utiliza como inicio del proceso de autenticación. En general será una credencial basada en un factor “algo que se sabe” (contraseña de usuario) que puede validar el sistema mediante la conexión a un repositorio corporativo (AD/LDAP, etc.) o externalizarse mediante el uso de plug-ins.
- **Captura y análisis del contexto** basado en políticas que determinan qué información de contexto (dispositivo, localización, horario, frecuencias y correlaciones) se procesa para determinar el nivel de riesgo de la autenticación. La captura de esta información de contexto se orquesta exclusivamente desde el servidor usando mecanismos web (HTMLy JavaScript).
- **Biometría del comportamiento.** De forma imperceptible para el usuario, mientras teclea su nombre y contraseña, se capturan rasgos biométricos de comportamiento que se procesarán en el servidor para determinar si existe coincidencia o no con un patrón de tecleo previamente generado por el usuario. Este proceso también se realiza exclusivamente utilizando mecanismos web.
- **Dispositivos de confianza.** El sistema permite que el usuario confirme explícitamente que un dispositivo es personal y de confianza, de forma que dicho dispositivo sirva como factor “algo que se tiene”. TrustedX implementa un protocolo de doble-cookie de un solo uso que ayuda tanto en la identificación compleja del

dispositivo, en línea con la guía del Federal Financial Institutions Examination Council (FFIEC) estadounidense, como en la protección contra ataques de pharming.

- **Autenticación de servidor intuitiva.** En la mayoría de casos, el usuario medio que no tiene un perfil muy técnico es incapaz de discernir si la conexión es segura y se realiza con el servidor auténtico. La posibilidad de que el usuario personalice la interfaz del servidor le ayuda a reconocerlo y, por tanto, combate los ataques de phishing porque evita que entregue su credencial cuando no identifica claramente la imagen que espera.
- **Segunda línea de autenticación configurable**, que se ejecuta en función de la política adaptativa requerida, y del resultado del análisis del contexto y/o de la biometría del comportamiento. Al igual que la primera línea, la segunda puede ser conducida por el sistema mediante la conexión a un servidor de autenticación corporativo que ya se encuentre desplegado (vía RADIUS) o externalizarse mediante el uso de plug-ins.
- **Inicio de sesión único**. El sistema basa su single sign-on (SSO) en i) los niveles de seguridad del NIST (levels of assurance), y en ii) la acumulación de factores superados con éxito. Esto permite desplegar políticas de control de acceso adaptables al contexto del usuario maximizando la usabilidad a la vez que la seguridad.
- **Eventos e inteligencia**. El sistema genera eventos de cualquier actividad de autenticación que gestiona: diferentes líneas, procesado de factores, captura y análisis del contexto, etc. Estos eventos pueden analizarse y auditarse de forma centralizada a través de la consola gráfica, y también pueden enviarse a un sistema de Inteligencia externo que podrá aprovechar dicha información para generar correlaciones e informes de seguridad avanzados (p.ej. de cumplimiento de regulaciones), e incluso integrarse con fuentes externas de gestión del riesgo.
- **Integración directa** mediante tecnologías web HTML, JavaScript y APIs REST. El sistema soporta los estándares OAuth 2.0 y SAML 2.0 para cumplir los roles de Servidor de Autorización y/o Proveedor de Identidad. A través de conectores se puede integrar la autenticación adaptativa en sistemas de control de acceso tales como CAS, IBM Security Access Manager o CA SiteMinder.
- **Adopción de nuevos mecanismos de autenticación**. Diseñado para la extensión, mediante plug-ins, a cualquier mecanismo actual o futuro para la primera o la segunda línea de autenticación, por ejemplo, PKI, tokens OTP, out-of-band OTP (SMS, email), etc..
- **Recomendaciones, guías y regulaciones**. El sistema observa las principales referencias en autenticación, a destacar: las guías NIST 800-63-1 y ITU-T X.1254/ISO/IEC 29115; el Esquema Nacional de Seguridad (ENS); la guía Authentication in an Internet Banking Environment de FFIEC, y otras fuentes como Cloud Security Alliance (CSA).



Etapas Autenticación Adaptativa

Escenarios de uso

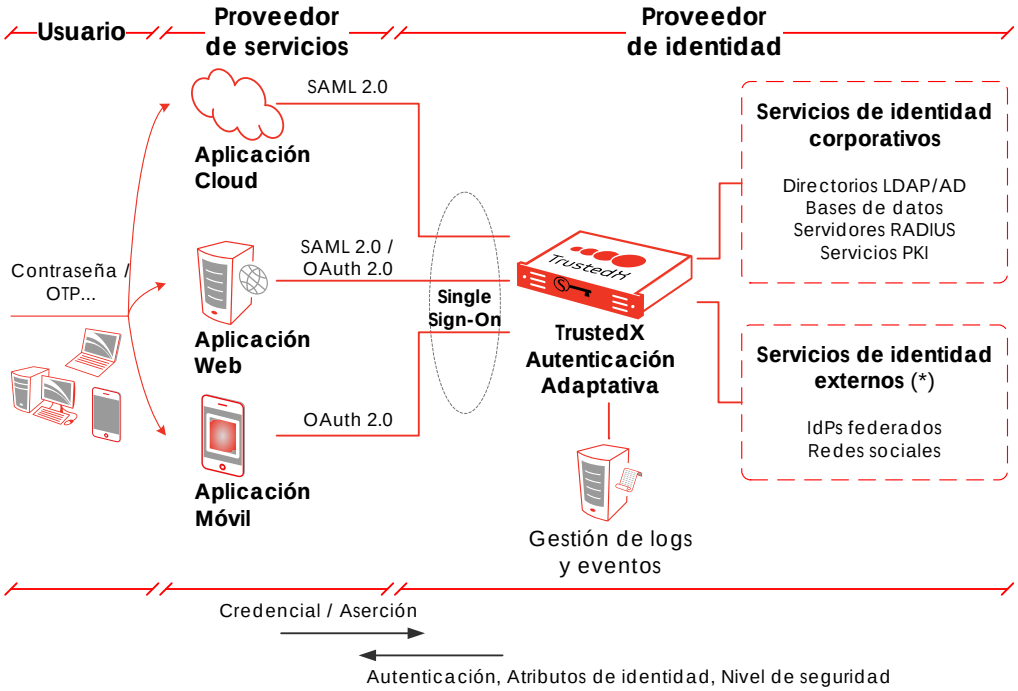
TrustedX Autenticación Adaptativa es un componente tecnológico orientado esencialmente al mundo web del que las tecnologías cloud, de movilidad y sociales estiran fuertemente. Estas tecnologías están presentes ya en todo el ecosistema TIC y abarcan todas las comunidades de usuarios: empleados con ubicación estable o móvil, con acceso a aplicaciones propias y como servicio en la nube; consumidores cada vez más habituados al comercio electrónico; administraciones públicas motivadas a ofrecer mejores servicios para el ciudadano, etc. El nexo común de todos estos ejemplos es la tendencia a la movilidad, el consumo de servicios en la nube y la integración de las redes sociales en todas las actividades. Por ejemplo, si un empleado ya está conectado a su cuenta de Facebook o Google, la empresa en la que trabaja podría dar acceso transparente a la agenda corporativa a una aplicación del usuario que se ejecuta en su dispositivo habitual.

Gracias al uso masivo de las tecnologías y los estándares web es posible crear una experiencia de usuario sencilla y uniforme independientemente del dispositivo que esté

utilizando–desktop, tableta, smartphone, smart TV, videoconsola…–, de la aplicación que esté accediendo –una aplicación corporativa alojada en sus instalaciones, un servicio en la nube, o una aplicación privada–, y de qué identidad esté usando de las múltiples posibles que posee –corporativas o sociales.

Mediante un sistema basado en políticas, TrustedX hace de árbitro y adapta el nivel de seguridad de cada autenticación al nivel exigido en el escenario, a partir de la evaluación del riesgo y solicitando factores adicionales cuando es necesario. TrustedX crea una experiencia SSO web basada en el riesgo para cualquier dispositivo y entorno de aplicación que soporte los estándares web. Y en especial vale la pena mencionar:

- **Cloud Access Management y SSO.** Gracias a la incorporación del estándar SAML 2.0, las organizaciones pueden autenticar a sus usuarios que se conectan a los proveedores de aplicaciones empresariales en la nube como Salesforce, Google, etc.
- **Mobile awareness.** Todos los teléfonos inteligentes y tabletas actuales disponen de navegador con soporte de los estándares web. Además, de forma nativa estos sistemas también disponen de motores que permiten la integración de las tecnologías web en las aplicaciones nativas. En el entorno móvil deben tenerse en cuenta ciertas peculiaridades y limitaciones a las que debemos adaptarnos; por ejemplo, si la captura del ritmo de tecleo no resulta conveniente porque resulta difícil teclear contraseñas en una pantalla táctil, este factor debe sustituirse por una biometría basada en el reconocimiento de los trazos y los gestos del usuario.



Autenticación Adaptativa

Integración

La propuesta de autenticación web de TrustedX es horizontal, y puede desplegarse en cualquier entorno: en todas las empresas y corporaciones, en la administración pública y en los portales de servicios que ofrezcan valor a sus usuarios (empleados, partners, ciudadanos y consumidores) a través de la web. Hoy en día, mucho del valor añadido pasa por integrar otros servicios de la nube, permitir un acceso cómodo independientemente del dispositivo, y aprovechar el tirón de las redes sociales. Pero esta integración siempre debe llevarse a cabo con las máximas garantías de seguridad, y procurando que el usuario goce de la mejor experiencia de acceso, condición necesaria para retenerlo.

Una oferta completa de autenticación

Safelayer es un fabricante de productos de alta seguridad. Históricamente hemos basado nuestra oferta en la tecnología PKI, que es la que ofrece los niveles de confianza más altos. Ahora, con las nuevas funciones de autenticación de TrustedX, la plataforma se potencia con un conjunto de mecanismos de autenticación que aportan niveles de confianza altos a la vez que ofrecen un equilibrio eficaz entre seguridad, coste y usabilidad.

Gracias a la incorporación de la autenticación adaptativa, la solución de Safelayer se convierte en una propuesta muy completa en materia de autenticación segura. Sin interferir en la experiencia de usuario, la combinación de factores de autenticación que consigue TrustedX aporta una mayor precisión en la autenticación y complementa el mecanismo más utilizado, la contraseña de usuario, con información contextual y biometría del comportamiento. El resultado es que el proceso de cada autenticación puede adaptarse al nivel de riesgo sin reducir el nivel de seguridad.