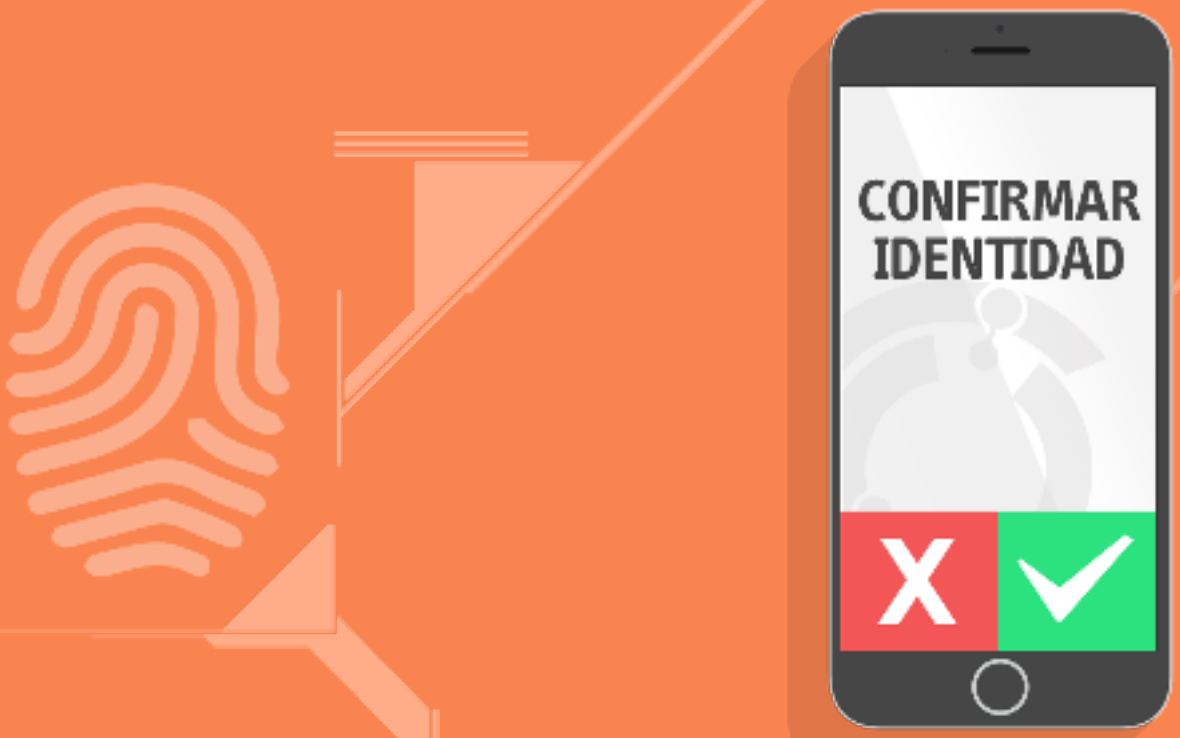
VU Mobile Tokens®



VU Mobile Tokens

Es la primera solución en brindar un esquema flexible, sencillo de utilizar, simple de implementar y de fácil distribución al momento de instaurar un sistema de doble factor de autenticación. Utiliza como soporte de hardware el teléfono celular del cliente. De esta forma los usuarios finales tienen la garantía de que ninguna persona mal intencionada podrá capturar sus credenciales para luego utilizarlas en un fraude o robo de información bancaria (*phishing*).

¿Qué es un sistema de doble factor de autenticación basado en dispositivos móviles?

Es una aplicación multiplataforma con soporte para J2ME, iOS (AppIe), Android, Blackberry, USSD y SMS que genera una contraseña de una única vez. La misma trabaja en conjunto con un módulo servidor que permite implementar un sistema de autenticación segura, y sin conexión directa entre el módulo usuario y el módulo servidor.

¿Dónde se instala?

EI módulo VU App & Cloud Server se puede implementar en cualquier tipo de entorno tecnológico debido a que es multiplataforma y provee una amplia capacidad de integración; ya sea a través de SOA, Radius o utilizando API's de integración a medida. Creado con ambientes de gran escala en mente, la solución posee una arquitectura distribuida que permite escalabilidad, alta disponibilidad y un sistema tolerante a fallos de forma sencilla y segura. Además, el *expertise* del equipo de desarrollo de VU permite integrar la solución en prácticamente cualquier ambiente tecnológico.

¿Cómo funciona?

VU Mobile Tokens permite generar una contraseña de única vez (OTP) en un teléfono celular, smartphone o dispositivo móvil compatible a través de cada uno de los Markets. Cuando el usuario necesita ingresar a un sistema, utiliza Ia contraseña (OTP) generada en su dispositivo personal, además de su contraseña estática, garantizando así que el individuo es quien dice ser.

VU Mobile Tokens

Avala la identidad del usuario, utilizando un segundo factor de autenticación de simple implementación y distribución que garantiza la seguridad robusta del usuario al generar una contraseña que es válida por única vez (OTP).

VU Mobile Multi Token

Cumple la funcionalidad de VU Mobile Tokens con la posibilidad de integrar múltiples tokens en una misma aplicación. Esto brinda al usuario la comodidad de tener centralizados todos sus sistemas de identicación un un solo lugar. La aplicación soporta múltiples VUID's y múltiples servicios de validación (VPN, Web, eBanking, IVR).

VU Mobile Challenge Response

Mediante la implementación del cliente VU Mobile Challenge Response, el sistema de autenticación contará con la implementación de un sistema de OTP que necesitara de un código entregado por el servidor para poder calcular cada OTP.

VU SMS Token

Permite el envío de la contraseña de única vez a través de SMS (Short Messaging Services) al 100% de los dispositivos móviles seleccionados. El servicio puede trabajar en modo simple vía; el usuario solo recibe la contraseña de única vez o en modo doble vía en la cual el usuario recibe un código y debe enviar otro por SMS para terminar el proceso de validación. Este módulo puede integrarse también a través de USSD.

VU Sync Token

Es la evolución en validación de identidades en Internet. Con esta solución los usuarios de sistemas informáticos no van a tener que preocuparse por ingresar complejos códigos o recordar extensas contraseñas. Con VU Sync Token solo basta con "Autorizar" cada transacción y el dispositivo móvil se encarga del establecer una comunicación segura. Por ejemplo, con su banco, y verifica que se den las condiciones para realizar dicha transacción minimizando la posibilidad fraude o robo de identidad.

Implementación de HOTP

Las soluciones de VU implementan las especificaciones del algoritmo HOTP. HOTP es un algoritmo generador de contraseñas de única vez, basado en HMAC especificado por la IETF. Como una regla general, en VU trabajamos basados en estándares y especi ficaciones avaladas a nivel mundial.

Especificación Técnica: RFC 4226
http://tools.ietf.org/htmI/rfc4226

Implementación de TOTP:

TOPT (Time Based One Time Password): por sus siglas en inglés Time Based One Time Password Algorithm es una extensión del ya probado algoritmo HMAC-Based one Time password. TOPT utiliza un esquema de implementación mediante el cuaI permite darle un tiempo corto de vida a cada OTP.

Especificación Técnica: RFC 6238
http://tools.ietf.org/htmI/rfc6238

Implementación de VUOTP:

VUOTP (VU One Time Password): VU cuenta con un método de generación, validación y autenticación de OTP's propietarios, mediante el cual permite trabajar de forma simultánea con un sistema por eventos, por tiempo y por patrones de autenticación. Esta modalidad otorga aI cliente Ia posibilidad de optar por una amplia variedad de opciones y generar así su propio esquema de autenticación robusta.

Implementación OATH:

OATH: Sistema de autenticación abierto, que permite a proveedores de soluciones robustas de autenticación convivir bajo una misma infraesctructura.
Las soluciones de VU Security son compatibles con dicho estándar Io que le permite integrarse con otras marcas y soluciones existentes en el mercado.

Especificación Técnica: Release 2.0
http://www.openauthentication.org/webfm_send/1

Personalización de algoritmo

VU se diferencia de otras soluciones en el mercado por tener la capacidad de personalizar el algoritmo para uso exclusivo del cliente. De esta manera se puede contar con un SEED único en el mundo que minimiza riesgos de explotación de vulnerabilidades.

Diferenciales

Multi Token: sólo un token para todas las aplicaciones remotas.

Intuitivo: el usuario solo tiene que ingresar el Phone PIN y aguardar a que automáticamente la aplicación le otorgue una contraseña por única vez (OTP).

Sin límites: Funciona en cualquier dispositivo que soporte J2ME, iOS, Android, Blackberry y USSD.

Práctico: evita al usuario demoras en utilizar sus sistemas ya que no depende de redes de telefonía celular, Internet o mensajes de texto para la generación y envío del token.

Económico: Al trabajar 100% en forma digital la reposición de cada mobile token es simple, gratis, rápida y amigable para cualquier usuario que haya olvidado, perdido o roto su dispositivo móvil.

VU

VU es una compañía especializada en el desarrollo de software de ciberseguridad, con foco en la prevención del fraude y el robo de identidad. Su misión es entregar experiencias digitales sin fricción y seguras tanto para ciudadanos, como para compañías.

Todas sus soluciones están destinadas al ámbito corporativo, usuario final y organismos gubernamentales y se basan en la evaluación del comportamiento de los usuarios con el fin de protegerlos contra ataques dirigidos, *pharming*, *phishing*, m*an in the middle*, *vishing* y *botnets*.

Es la única empresa de la región alineada a las buenas prácticas en materia de autenticación internacional, miembro de FIDO Alliance, OATh y OIC. Fundada en 2007, cuenta con oficinas en Argentina, Chile, Uruguay, Ecuador, Colombia, Costa Rica, México y Perú.

Capacidad de innovación

Desde sus inicios los fundadores de Ia empresa se enfocaron en desarrollar soluciones tecnológicas que se adapten a las necesidades de los usuarios, simplificando y exibilizando su utilización con fines de seguridad.

Escenarios de implementación

Las soluciones de VU pueden integrarse dentro de cualquier proceso de autenticación o validación de operaciones que utilice sistemas informáticos. Algunos de los más comunes y utilizados diariamente son: Sistemas de pagos y financieros, Acceso a redes corpora vas, sistemas contables, accesos VPN's, Intranets, correo electrónico, Home Banking, si os Web, Sistemas de seguridad física (molinetes, accesos a bóvedas) o cajeros automáticos, CRMs, y/o IVRs. Fabricantes como Cisco Systems, Juniper, Citrix, For net y Microsoft, entre otros recomiendan y certifican las soluciones de VU .