

SCANNING ...



The Smart Move

► Suite de Autenticación de NETteller Autenticación de 2 Factores vía Dispositivo Móvil y/o Token OTP

DEFINICIÓN

Autenticación de 2 Factores se refiere a un proceso de seguridad en el que el usuario dispone de dos medios de identificación; los cuales suelen ser sistemas basados en algo poseído, como un Token o una tarjeta inteligente y sistemas basados en algo conocido, como un ID o un password.

Por qué Autenticación de 2 Factores?

Una autenticación de 2-factores puede reducir drásticamente la incidencia de robo de identidad, phishing y otros fraudes en Internet puesto que los delincuentes necesitan algo más que el código de seguridad para tener acceso a la información.

Usar más de un medio de autenticación también se conoce como autenticación fuerte; mientras que usar un solo medio, se considera autenticación débil, por ejemplo el código de seguridad.

Que es la Suite de Autenticación de NETteller?

Es un servidor de autenticación de contraseñas a través de un dispositivo móvil o un Token que le permite a los e-business mejorar su seguridad fácil y rápidamente, a menores costos y con bajos riesgos de implementación.

El servidor de autenticación de NETteller logra esto con una solución innovadora la cual protege el acceso a los servicios de Internet a través de la autenticación de 2 - factores, aprovechando los teléfonos celulares y/o Token OTP. La solución de autenticación de NETteller sirve para sobrepasar los temas de seguridad en Internet/Intranet, permitiendo al usuario autenticarse a si mismo usando su propio teléfono celular o el Token de NETinfo.

Internet Bancario y el Servidor de Autenticación de NETinfo

Es un gran problema para los bancos identificar al cliente adecuado que utiliza sus servicios de banca electrónica. El fraude en línea ha ido en aumento con los años a cifras alarmantes, sin embargo

hay muchas maneras de mejorar la seguridad de las transacciones en línea. Algunas de ellas es el uso de SMS TAN (teléfono móvil) o un Token OTP las cuales podrían reducir el riesgo de las operaciones, de una forma más rentable y conveniente.

SMS TAN y Token OTP: dos opciones de autenticación en sólo un paquete.

Autenticación SMS

La autenticación a través de mensajes de texto (SMS) permite enviar un mensaje al celular del cliente que está haciendo una operación en Internet. En éste mensaje el cliente recibe un código para que sea digitado en la Banca de Internet como parte del procesamiento de la operación. Como idea, no puede ser más sencilla:

- Los usuarios de Banca Móvil no necesitan instalar un software en su dispositivo móvil .
- El código TAN es generado por el servidor de Autenticación de NETinfo y es válido sólo para un tiempo específico y transacciones específicas.
- Los usuarios necesitan tener el celular a la mano si quieren hacer una transacción que requiera 2do factor de autenticación (clave dinámica).
- Al iniciar el uso de los servicios de Internet o al aprobar transacciones particulares, el usuario recibiría un mensaje con 8 dígitos, los cuales tienen que digitar en la transacción dentro de los siguientes x minutos para completar la transacción.

SMS TAN es fácil de implementar puesto que no es necesario instalar un Hardware o Software en el celular y así mismo es fácil de entender y usar.

Finalmente, es mucho más seguro que simplemente tener un usuario y una contraseña.



Autenticación Token OTP

Es un dispositivo electrónico, generador de contraseñas dinámicas "OTP" que se le da a un usuario autorizado diseñado para facilitar el proceso de autenticación. Este está totalmente integrado con el Servidor de Autenticación de NETInfo como una alternativa SMS TAN, dándole flexibilidad al usuario para usar SMS TAN o el OTP Token.

Cuando un usuario decide usar el modo de autenticación OTP Token, debe ingresar los seis dígitos dinámicos en la pantalla del sistema a autenticar. La clave cambia cada 60 segundos con el objetivo de garantizar una mayor seguridad. No es necesario presionar ningún botón; un Token es muy fácil y simple de usar.



Características del Token OTP de NETInfo

Tamaño:	55 x 25 x 9 mm
Pantalla	LCD de 8 caracteres
Cambio/Renovación de la clave:	Cada 60 segundos
Temperatura de Funcionamiento:	-40 a 100 Grados Celsius
Humedad:	Resistencia al Agua
Duración:	4,5 Años
Resistencia	Puede ser lanzado desde una altura de 15 mts.

oath
initiative for open authentication

NETInfo Plc

Casa Matriz:
Street 37 Stasicratous, 1ª Planta
1065 Nicosia, PO Box 22658
Tel: +357 22 753636
Fax: +357 22 765680
URL: www.netinfo.eu,
e-mail: netteller@netinfo.eu

Oficina Regional:
Calle 31 N. 13A - 51, Ofc: 213,
Bogotá, Colombia
Tel: (57)+1 4759466



www.netteller.eu

Servidor de Autenticación de NETInfo

Ingreso de Transacción

El Usuario ingresa la transacción



Pantalla de pre-Confirmación

El usuario visualiza una pantalla de pre-confirmación con todos los detalles de la transacción.



Autenticación de 2 Factores

Selecciona el Método de Autenticación

OTP Token

Lea los seis dígitos de la contraseña (Token)



Celular (Mobile device)

El Servidor de Autenticación de NETInfo, verifica el ID del usuario, si es válido genera un número de ocho dígitos (Número de Autorización de Transacción).



6 Dígitos OTP:

CONFIRM

El usuario necesita ingresar los 6 Dígitos OTP y confirmar la transacción.



MENSAJE DE OCHO DÍGITOS
El usuario recibe un mensaje de texto con ocho dígitos.

8 digit TAN



8 dígitos TAN:

CONFIRM

El usuario necesita ingresar el TAN de 8 dígitos dentro del tiempo limite especificado (2-5 min) y confirmar la transacción.

Autenticación de Usuario

El servidor de autenticación de NETInfo autentica el usuario y acepta la transacción.

