

VENTAJAS

Va más allá de la autenticación

Mobile Authenticator Studio de OneSpan va más allá de la autenticación para garantizar que la aplicación que se ejecute en el teléfono se proteja automáticamente durante el tiempo de ejecución de la aplicación. Nuestra seguridad de aplicación incluye las siguientes características:

- Detección de liberación y rooteo
- Endurecimiento de la seguridad de la aplicación
- Vinculación de dispositivos
- Comunicación segura del canal
- Análisis de riesgo optimizado
- Anticlونación

MOBILE AUTHENTICATOR STUDIO

La seguridad se combina con la comodidad: la seguridad de las aplicaciones móviles optimizada se combina con una experiencia de usuario sin fricción

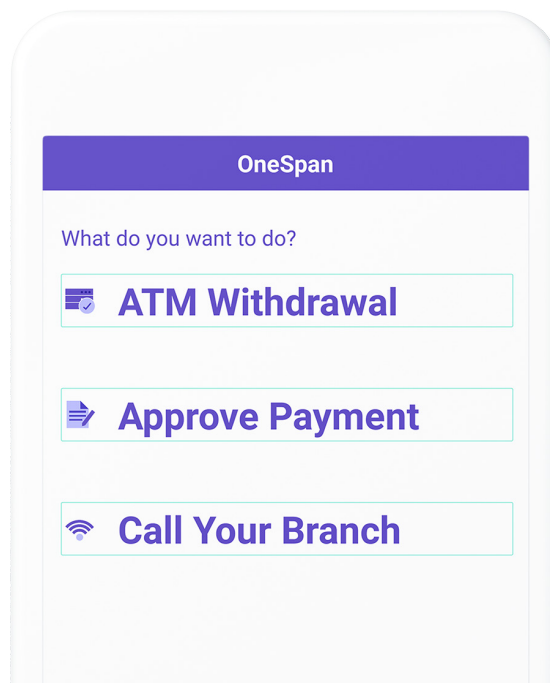
Los bancos, instituciones financieras y empresas que ofrecen aplicaciones en línea y móviles enfrentan múltiples desafíos. Las aplicaciones en línea y móviles son altamente susceptibles a los ataques cibernéticos y al fraude, que en los últimos años se han vuelto cada vez más sofisticados. Al mismo tiempo, la adopción de aplicaciones móviles depende de una experiencia intuitiva y sin inconvenientes para los usuarios. ¿Cómo garantiza la seguridad de su aplicación móvil mientras la mantiene conveniente y transparente para sus usuarios móviles?



Las soluciones de OneSpan se diferencian de las soluciones de otros proveedores porque la solución es fácil e intuitiva de usar. En particular, nos gustó el enfoque simple aplicado a los tokens para dispositivos móviles. La implementación de la nueva solución fue rápida y eficiente, y confiamos en la capacidad de OneSpan para respaldar la implementación con el mínimo esfuerzo”.

Chris White
Chief Information Officer
Clyde & Co

Mobile Authenticator Studio de OneSpan equilibra la necesidad de una mayor seguridad de las aplicaciones con las demandas de conveniencia para el usuario al brindar una seguridad integral e integrada para sus aplicaciones móviles, combinada con una experiencia de autenticación y firma electrónica “sin manos” y sin fricción para sus usuarios móviles. Y cuando se combina con Mobile Security Suite de OneSpan, ofrece un marco de seguridad integral e integrado para sus aplicaciones móviles.



Seguridad de aplicaciones optimizada

Para cualquier aplicación móvil, la creación de un entorno seguro para el proceso de autenticación del usuario es fundamental. Es por eso que Mobile Authenticator Studio va más allá de la autenticación para garantizar que cualquier aplicación que se ejecute en una plataforma móvil esté auto-protegida en todos los aspectos del tiempo de ejecución de la aplicación:

Detección de liberación y rooteo: Garantiza la seguridad de las plataformas móviles al detectar si hay evidencia de liberación o rooteo, por lo que puede tomar las medidas adecuadas en función de sus políticas de seguridad.

Endurecimiento de la seguridad de la aplicación: Soporta las mejores técnicas de endurecimiento de su clase, como la reducción a cero de la memoria, la protección de ingeniería inversa, el almacenamiento seguro y la criptografía de caja blanca para mantener a las aplicaciones y los usuarios a salvo de posibles ataques.

Vinculación de dispositivos: Vincula de manera segura a un usuario autorizado con sus dispositivos autorizados para poder prevenir la clonación o reutilización de claves criptográficas. La aplicación Mobile Authenticator Studio también está vinculada a componentes dependientes del dispositivo y enlazada al usuario a través de un código PIN seguro.

Comunicaciones seguras del canal: Asegura la integridad de las transacciones digitales al proporcionar un canal seguro encriptado, independiente y multiplataforma entre el servidor y el dispositivo cliente, de modo que solo los dispositivos autorizados para recibir información de la transacción podrán descifrarla y firmarla.

Análisis de riesgo optimizado: Ofrece capacidades de puntuación de riesgo únicas que están integradas en los procesos de autenticación y firma basados en los elementos del usuario, la plataforma y el contexto de la aplicación, brindando una mayor protección, así como también un análisis de riesgo del lado del servidor.

Anti-clonación: Para los sistemas operativos, OneSpan respalda la protección del almacenamiento seguro a través de la función del componente de seguridad del dispositivo. La seguridad de los datos en los teléfonos Android habilitados se logra a través de un segundo nivel de cifrado, lo que proporciona una excelente defensa contra ataques de clonación de aplicaciones ya que la clave de cifrado almacenada en el componente de seguridad no se puede extraer.

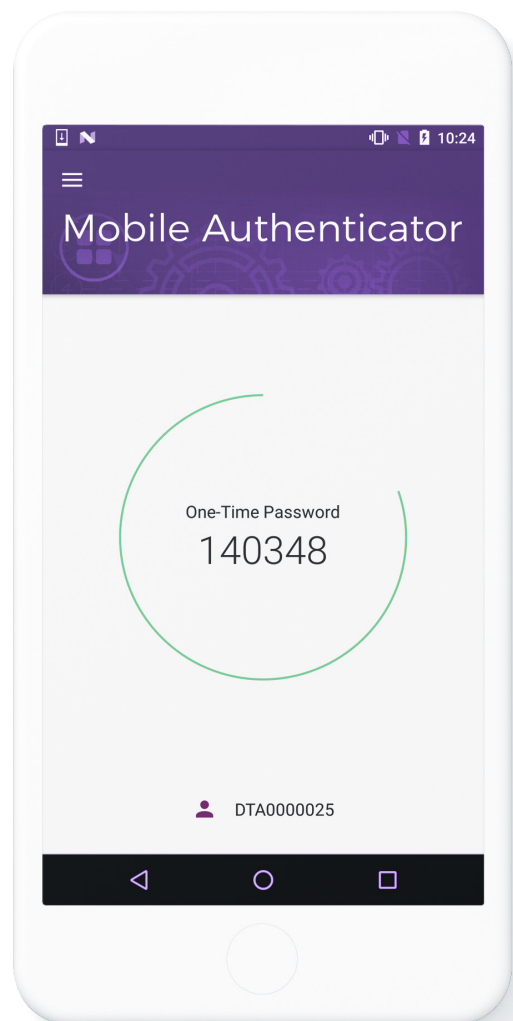
Experiencia de usuario transparente

Cuando se trata de la adopción por parte del usuario de su aplicación móvil, la experiencia del usuario a menudo puede ser un factor determinante en su éxito o fracaso. Mobile Authenticator Studio ofrece opciones de autenticación de dos factores convenientes y fáciles de usar y opciones de firma electrónica que eliminan la fricción de seguridad de la ecuación:

- **Escaneo del código QR:** Los usuarios simplemente capturan el código QR con un dispositivo móvil, ingresan un código PIN y pueden iniciar sesión instantáneamente en una aplicación o validar una transacción. Se integra con la tecnología

patentada Crono® de OneSpan, así como con los códigos QR abiertos.

- **OTP transparente:** Ofrece autenticación y firma “manos libres” cuando un usuario está realizando una sesión en línea, y es lo suficientemente flexible como para proporcionar OTP transparente o generar una firma electrónica que se dirige automáticamente al servidor correspondiente. Para el usuario, esto significa que no es necesario escribir ninguna información, y una experiencia de autenticación segura y completamente libre de fricciones.
- **Soporte para múltiples dispositivos:** Asegura que un usuario pueda aprovechar de forma segura cualquier dispositivo registrado previamente para la autenticación de la aplicación y la firma de transacciones, independientemente de la plataforma. Las capacidades de canal seguro aseguran que la información cifrada enviada desde el servidor solo pueda ser descifrada y accedida por el conjunto de dispositivos autorizados previamente para ese usuario.
- **Seguridad entre aplicaciones:** Entre las aplicaciones, Mobile Authenticator Studio realizará las comprobaciones de seguridad necesarias, generará la OTP y la pasará directamente al servidor correspondiente, de modo que el usuario pueda establecer instantáneamente un acceso seguro para prácticamente cualquier aplicación en el lado del cliente.



ESPECIFICACIONES TÉCNICAS

Solo respuesta	<ul style="list-style-type: none">· Solo tiempo, solo evento o tiempo + basado en evento· Algoritmo de cifrado AES / Triple DES· Respuesta: 6 a 16 decimales/ hexadecimales· Dígito de control· 256 segundos de paso de tiempo
Código de confirmación del anfitrión	<ul style="list-style-type: none">· AES / Triple DES· Longitud de 4 a 10 decimales/ hexadecimales (1 a 10 en modo desafío/ respuesta)
Desafío/Respuesta	<ul style="list-style-type: none">· Solo tiempo, solo evento o tiempo + basado en evento· Algoritmo de cifrado AES / Triple DES· Longitud de desafío de 4 a 16 decimales/ hexadecimales· Longitud de respuesta de 6 a 16 decimales· Dígito de control· 256 segundos de paso de tiempo
MAC/firma	<ul style="list-style-type: none">· Solo tiempo, solo evento o tiempo + basado en evento· Algoritmo de cifrado AES / Triple DES· Longitud de 4 a 16 decimales/ hexadecimales· Hasta 8 campos de datos personalizables· Longitud de campo de datos de 4 a 16 dígitos· 256 segundos de paso de tiempo



OneSpan permite a instituciones financieras y otras empresas triunfar mediante grandes avances en su transformación digital. Lo logramos generando confianza en las identidades personales, los dispositivos que usan y las transacciones que definen sus vidas. Creemos que esta es la base para mejorar y hacer crecer las empresas. Más de 10 000 clientes, entre los que se incluyen más de la mitad de los 100 mejores bancos a nivel global, confían en las soluciones de OneSpan para proteger sus relaciones y procesos empresariales más importantes. La solución unificada y abierta de OneSpan reduce los costes, acelera la captación de clientes y aumenta la satisfacción de los clientes en ámbitos que van desde la integración digital hasta la reducción del fraude, pasando por la gestión del flujo de trabajo.



Copyright © 2018 OneSpan North America Inc., todos los derechos reservados. OneSpan™, DIGIPASS® y CRONTO® son marcas comerciales registradas o no registradas de OneSpan North America Inc. y/o OneSpan International GmbH en los Estados Unidos y otros países. El resto de marcas comerciales o nombres comerciales son propiedad de sus respectivos dueños. OneSpan se reserva el derecho de realizar cambios en las especificaciones en cualquier momento y sin previo aviso. La información proporcionada por OneSpan en este documento se considera exacta y fiable. Sin embargo, OneSpan no se hace responsable de su uso ni de la infracción de patentes u otros derechos de terceros resultantes de su uso. Última actualización: **noviembre del 2018**.

CONTÁCTENOS

Para más información:

info@OneSpan.com

www.OneSpan.com