

DetectID®

Aproveche los Dispositivos Móviles
y Asegure Todos los Canales

Con cada vez mayor frecuencia, los clientes bancarios prefieren utilizar sus dispositivos móviles para manejar sus cuentas, y esto está haciendo que los bancos impulsen la transformación digital en todos los canales. Sin embargo, el crecimiento de la banca online y móvil también ha producido un aumento en el número de ciberataques, el cual ha erosionado la confianza de los usuarios y ha elevado el riesgo de fraude. Las soluciones tradicionales no han sido capaces de mantener el ritmo de las amenazas: las contraseñas ya no son seguras, los mensajes SMS son altamente vulnerables, y los tokens son demasiado costosos e inconvenientes para ser distribuidos masivamente. Evolucione a un sistema de autenticación moderno que ofrezca el balance justo entre seguridad fuerte y una experiencia de uso sin fricción. DetectID permite que sus clientes utilicen sus teléfonos móviles para proteger sus interacciones en cualquier canal bancario.

Los Beneficios de la Autenticación Móvil



Agilice la autenticación de usuarios y reduzca los costos

Unifique todos los componentes de su estrategia y gestione los factores de autenticación desde un solo panel. Aproveche los teléfonos de sus usuarios para reducir los costos de distribución y dejar atrás los tokens y los mensajes SMS.



Proteja el canal móvil

La tecnología móvil está invadiendo al mundo, y las transacciones en este canal continúan creciendo a un ritmo asombroso. Implemente autenticación fuerte y firmado de transacciones en todas las actividades financieras realizadas en dispositivos móviles.



Manténgase competitivo a través de la seguridad multinivel

La industria financiera se encuentra en plena transformación, y las instituciones deben innovar para mantenerse al día. Una estrategia de seguridad multinivel que cubra todas las etapas del ciclo de vida del fraude es crucial para fortalecer la confianza de los usuarios y tomarle la delantera al cibercrimen.



Ofrezca una mejor experiencia a sus usuarios finales sin sacrificar la protección

No obligue a sus clientes a superar incontables obstáculos para mantener seguras sus interacciones financieras. La reducción de la fricción en lo concerniente a la seguridad incrementa el volumen de transacciones, mejora las relaciones con los usuarios y crea lealtad por medio de la conveniencia.

Desatando el Poder de la Autenticación Móvil

Autenticación con solo un toque en la pantalla

Sin necesidad de esperar llamadas telefónicas o ingresar códigos, los usuarios simplemente tocan la pantalla de sus dispositivos para autenticarse. Los mensajes son enviados a través de un canal de comunicaciones cifrado que resiste ataques y soporta el firmado transaccional. Esta tecnología puede ser utilizada en diversos casos, incluyendo verificación de transacciones basada en riesgo, alertas de fraude, transacciones sin tarjeta presente, confirmación de operaciones, recordatorios o notificaciones para clientes, y muchos más.

Flujo de la autenticación push



Conveniente experiencia de uso con biometría

Los factores biométricos de rostro, voz y huella dactilar pueden ser aprovechados por la tecnología presente en los teléfonos móviles para integrar las características físicas de los usuarios en la estrategia de autenticación. Combine la biometría con otros factores para controlar el volumen de alertas y reducir los falsos positivos.

Factores biométricos de autenticación



OTPs digitales

Reemplace fácilmente los tokens físicos con tokens digitales que brindan una mejor experiencia de uso sin tener que ser distribuidos físicamente. Las contraseñas de un solo uso basadas en software validan inicios de sesión y actividad transaccional mediante el estándar OATH de códigos de tiempo para un solo uso. Además, esta solución soporta múltiples identidades en una misma aplicación. Los OTPs digitales se encuentran disponibles para Apple iOS y Android.

SDK para autenticación nativa

Proteja la identidad de sus usuarios sin hacerlos descargar aplicaciones de terceros. Inserte autenticación transparente en su propia aplicación móvil a través del Kit de Desarrollo de Software (SDK) de DetectID, el cual suministra autenticación push desde las mismas aplicaciones nativas.

Características de DetectID

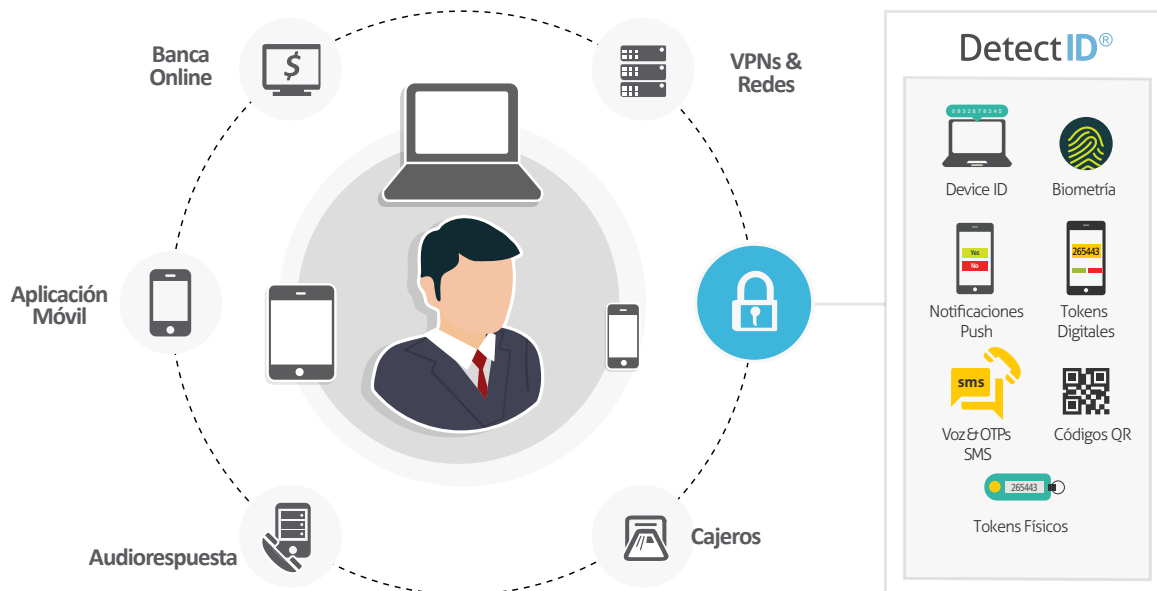
Seguridad de aplicaciones móviles que garantiza dispositivos confiables

Actualmente las plataformas móviles son el núcleo de la interacción con sus clientes, y proteger su aplicación contra el malware y otros ataques es crucial. El SDK de DetectID integra protección de aplicaciones móviles que permite identificar dispositivos confiables o sospechosos, detectar procesos de "jailbreak", e incrementar la seguridad contra ataques Man-in-the-Middle, aplicaciones falsas y pharming.

Los factores de autenticación móvil de DetectID son soportados por un flexible e innovador marco multifactorial, el cual incluye la mejor tecnología de huellas de dispositivo de su clase, y ofrece una experiencia de uso basada en riesgo y sin fricción.

Avanzado reconocimiento de dispositivos

La generación dinámica de huellas digitales de navegador reconoce con precisión dispositivos recurrentes enfocándose en los atributos realmente importantes y no en el contexto o los cambios en la configuración. Esta tecnología de reconocimiento de dispositivos sin cookies minimiza las tasas de colisión y fricción mientras opera de forma transparente a los usuarios finales.



Altamente escalable:

Soporte para millones de usuarios con la posibilidad de añadir más en cualquier momento y sin impacto alguno.

Flexible integración y administración:

- Despliegue paralelo con soluciones de autenticación existentes para una migración sin esfuerzo.
- Sencilla integración y APIs fáciles de usar para auto-gestión, incluyendo aprovisionamiento y activación de dispositivos, aplicaciones federadas, y servicios basados en la nube (p.ej: Salesforce.com, Microsoft 365, etc.).

Asiste a las organizaciones en el cumplimiento de importantes regulaciones emitidas por:

- Concejo Federal de Evaluación de Instituciones Financieras (FFIEC) Manual de Evaluación de Tecnologías de la Información (IT Handbook) – Manual de Sistemas de Pagos Retail, Apéndice E: Servicios Financieros Móviles.
- Instituto Nacional de Estándares y Tecnología (NIST) Parámetros de Identidad Digital, Publicación Especial 800-63B: Gestión de Autenticación y Ciclo de Vida.
- Estándares Técnicos Regulatorios sobre Autenticación Fuerte de Usuarios y Comunicaciones Comunes Seguras de la Autoridad Bancaria Europea (EBA) bajo el Artículo 97/98 de la Directiva 2015/2366 (también conocida como Directiva de Servicios de Pago (PSD2)).