IDVision with iovation

Product Sheet

LaunchKey Multifactor Authentication

LaunchKey provides users with a variety of authentication options through a mobile authenticator embedded within a mobile application.

Finding a comprehensive solution for multifactor authentication and real-time authorization – one that offers multiple authentication methods, is secure by design, and supports a broader risk-based approach – is a top priority for companies seeking strong security with a better user experience.

LaunchKey is a comprehensive MFA solution that extends the authentication capabilities of mobile devices that consumers already own. LaunchKey leverages the technologies incorporated into mobile devices for powerful authentication that's more secure, easier to use, and more flexible than its predecessors.

With a variety of authentication options provided through a mobile authenticator embedded within your mobile app consumers can employ strong authentication right in your app, leveraging all three types of authentication factors: something you know (knowledge), something you have (possession), and something you are (inherence). Available methods include: fingerprint recognition, facial recognition, device recognition, Bluetooth wearable factor, PIN code, pattern code and geofencing.

LaunchKey secures every consumer interaction, whether online or offline. Keep consumers safe at all touchpoints and provide a great experience.

Stop Account Takeover (ATO), While Improving the Consumer Experience

Mobile multifactor authentication allows you to secure all points of risk from ATO including login, account management and the contact center. Provide consumers a unified authentication experience across all customer channels, while reducing the use of more burdensome authentication methods such as one-time password (OTP) and knowledge-based authentication (KBA).

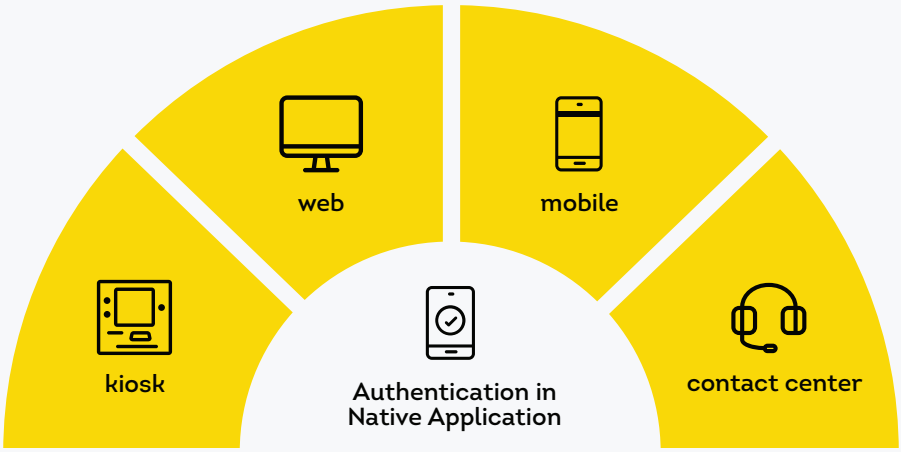
Go Beyond Alerts to Authorization

Send consumers all of the details they need to confidently authorize a transaction. They can quickly approve or deny wire transfers, large purchases or receipt of goods. Fight friendly fraud with a strong approval record that provides nonrepudiation.

Keep Customers In-App and Preserve Your Brand Equity

Unique to LaunchKey is a mobile authenticator that can be completely white-labeled and embedded within your own iOS and Android apps. Customers authenticate and authorize transactions right in your app, avoiding the need to send them out-of-app to higher-friction alternatives.

Provide omnichannel authentication for all customer interactions.



Key Features

GEO-FENCING

Leverage the enhanced geolocation capabilities of mobile devices to restrict authorization to specified locations or geographic territories.

OMNICHANNEL AUTHENTICATION

Give customers a single powerful authenticator to use across every touchpoint with your business whether online or offline. LaunchKey manages all authentication processes right in your mobile app.

UPDATABLE PLATFORM

LaunchKey uses the built-in features of mobile devices, making it easy to add additional authentication factors as they become available. New methods can be readily incorporated with a simple SDK update.

DECENTRALIZED, ANONYMOUS ARCHITECTURE

Older authentication systems use large centralized credential stores that are a lucrative target. We separate the authentication process from the application, keeping encrypted credentials distributed on each consumer's device to reduce risk and alleviate attack vectors.

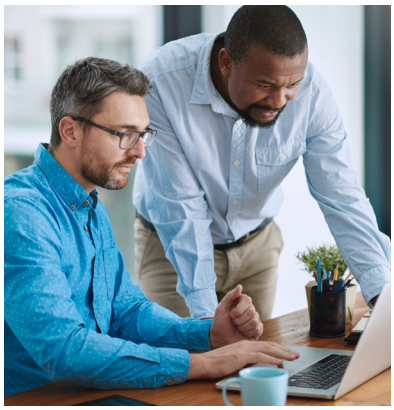
DYNAMIC SECURITY POLICIES

Programmatically adjust the level of security and assurance required at any given time with custom request rules to adjust to real-time risk insight and reduce customer challenges.

PLATFORM-AGNOSTIC

Leverage LaunchKey with virtually any online service. No matter what server platforms or authentication systems you have in place, LaunchKey is compatible and easy to integrate.

Key Advantages



Whether onboarding new users or resetting passwords, multifactor authentication allows for the global governance of any user attempting to access the identity management ecosystem.

Secure every point of the customer journey

Used in conjunction, iovation's solutions secure any point in the customer's online journey, from account creation to purchasing, to assure that consumers are identified correctly and fraud is stopped.

Authenticate in real time

In about 100ms, iovation recognizes a device, checks if it's authorized for an account and checks for risk signals. Identify and authenticate all device types, from phones and PCs to laptops and tablets, regardless of the platform, OS, browser or mobile apps.

99.9% uptime

iovation's distributed SaaS infrastructure supports the largest transaction volumes in the world with an average response time of 100 milliseconds. An active-active infrastructure means no service interruptions during updates or maintenance.

World-class fraud and ATO experts

Add our trusted fraud advisors to your team. Our customer success team partners with you to solve your unique business challenges and adapt to an ever-changing fraud environment.

Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit iovation.com

TransUnion
Formerly iovation

Portland Office
555 SW Oak Street, Suite #300
Portland, OR 97204 USA
PH +1 (503) 224 6010
EMAIL info@iovation.com

United Kingdom
PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation.com