iovation®

DATASHEET

iovation LaunchKey

Multifactor strength, single-factor usability

Finding a comprehensive solution for multifactor authentication – one that offers numerous MFA options, is inherently secure by design, and has the ability to interoperate seamlessly with other authentication solutions – is at the top of the list for companies seeking strong security that won't slow down their customers.

LaunchKey is a comprehensive solution that includes an intuitive mobile application and a number of built-in authentication factors that can be easily configured through the central server's dashboard.

Administrators of LaunchKey can determine which authentication factors to use for any access or authorization request within a site or application. For higher-risk activities, like fund transfers or adding new users to an account, they can even require two or three factors to be used in combination. Factors include:

Circle Code: Turn the touch display of your customer's mobile device into an interactive combination lock. Your customer sets the combination lock pattern, validates it, and then gains secure, memorable, passwordless access to your application.

PIN Codes: End users can create simple 4-digit PIN codes, and system administrators can determine when these need to be refreshed.

Bluetooth Proximity: Insure that a pre-selected, pre-paired Bluetooth® device – like a watch, Fitbit®, or another mobile device – is within close proximity whenever a user tries to authenticate.

Fingerprint Scan: Turn your end-user's sensor-equipped mobile device into a tool to validate fingerprints for authentication for your site.

One-Time Passwords: Create and manage one-time passwords using time-bound options that expire after a selected interval.

Additional Authentication and Authorization Controls

Beyond the strong authentication factors listed above, LaunchKey provides additional control factors that are easily enabled through an intuitive admin interface.

LaunchKey's Geofencing and Timefencing options treat the user's location or the time of login request as additional authentication constraints. Simply select a point from the map screen and then expand or zoom to determine the boundary of a Geofence. If time restrictions are also desired, select the time ranges where logins can be attempted. Any authentication attempts outside these geographic or temporal zones will be denied.

The "slide approval" capability allows an immediate, interactive response to an authorization request. This can be used to authorize a transaction that may be over a preset amount, or to provide an additional confirmation of risky activities like adding a new shipping address or requesting a fund transfer. Mission- and business-critical authorizations can be configured to require responses from two or more parties, providing additional security and traceability.

Customer Choice

Some of your customers are growing more savvy about their online security. Some actually want more authentication options than just usernames and passwords. LaunchKey provides an answer for them by allowing end-users to determine whether they want to enable additional factors, like PINs, as part of their sign-on process.

Another group of customers is less concerned about their online security and frequently reuses simple passwords. For them, you can force the use of an option like geofencing, or require another factor like a thumbprint or proximity to another Bluetooth device.

Implementation Options

LaunchKey comes with an off-the shelf, intuitive authenticator application for both iOS and Android, and a complete range of additional implementation and integration options.

With an option for White Label customization, subscribers can integrate the core features of LaunchKey capabilities into their own mobile apps and take advantage of their existing brand elements. This modal version of LaunchKey runs “above” your app and provides all the functionality and options of the off-the-shelf version of the authenticator app.

Complete SDK support for desktop and web application integration covers Python, Java, Ruby, and PHP, or developers can build mobile authenticator options into their own apps using Android, iOS or Windows Phone SDKs. Similarly, developers using Wordpress or Drupal can also utilize readily available plugin modules to replace their password-based authentication systems with LaunchKey’s intuitive multifactor options.

Security Protocols and Standards

LaunchKey has been designed with the latest and most extensible protocols in mind.

- **OAuth 2.0:** The latest evolution of the OAuth protocol originally created in 2006. OAuth 2.0 focuses on developer simplicity and provides specific authorization flows for web applications, desktop applications, mobile phones, and even Internet of Things (IoT) and living room devices.
- **OpenID:** A distributed identity protocol allowing webmasters to rely on trusted third parties for authentication. OpenID eliminates the need for webmasters to provide their own login systems, and allows users to log in to multiple websites without needing a separate identity and password for each.
- **SSH PAM:** For Unix systems, this pluggable authentication model allows a file and remote access model to work securely, even over unsecured networks.
- **Encryption:** LaunchKey uses public-key cryptography with 256-bit AES encryption. The latest version of LaunchKey authenticator app uses 4096-bit RSA keys for host devices.

Key Advantages

- ☑ **Works with iovation’s Customer Authentication service as part of a risk-based Dynamic Authentication Suite that provides the right level of authentication – at just the right time**
- ☑ **Provides multiple MFA options – from PINs to fingerprints to a graphic Circle Code – in one comprehensive package**
- ☑ **Authentication plus real-time authorization in an always-available online solution**
- ☑ **Includes fully extensible SDKs and APIs that make it easy for developers to build dynamic authentication into their own apps**
- ☑ **Allows end-user customers to select their authentication options within the boundaries set by the site or application administrator**

iovation®

Find out more at **www.iovation.com** or (503) 224-6010.