iovation LaunchKey

Increase security and provide customers with frictionless multifactor authentication

Finding a comprehensive solution for multifactor authentication – one that offers multiple authentication methods, is secure by design, and supports a broader risk-based approach – is at the top of the list for companies seeking strong security that won't slow down their customers in a post-password era.

LaunchKey is a comprehensive multifactor authentication (MFA) solution that extends the authentication capabilities of mobile devices that end users already own. Instead of relying on insecure passwords or cumbersome one-time passcodes, LaunchKey leverages the modern technologies incorporated into mobile devices for powerful authentication that's more secure, easier to use, and far more flexible than its predecessors.

True Multifactor Authentication

LaunchKey provides users with a variety of authentication options through a mobile authenticator embedded within a mobile application. Through these methods, users can employ strong authentication by leveraging all three available types of authentication factors: something you know (knowledge), something you have (possession), and something you are (inherence). Available authentication methods include:

Device Factor: Inherent to all LaunchKey authentication requests is identification of the mobile device on which the request is received.

Fingerprint Scan: Leverage the mobile device's embedded fingerprint scanner for biometric authentication.

Facial Scan: Use the mobile device's integrated facial recognition scanner for biometric authentication.

Geofencing: Verify that the mobile device is within geographic boundaries specified by the consumer or the requesting service.

Circle Code: Turn the touch display of your customer's mobile device into an interactive pattern code like that of a combination lock.

PIN Code: End users can create and change simple PIN codes like the codes they use to lock or unlock their mobile devices.

Wearable Factor: Insure that a pre-selected, pre-paired Bluetooth® device – like a watch, Fitbit®, or other device – is within proximity.

Since LaunchKey uses the built-in features of mobile devices, additional authentication factors can be added as they become available on the device.

LaunchKey empowers users to leverage the authentication methods that they're most comfortable with and which best fit their security needs. This choice helps to ensure maximum adoption of strong authentication by removing barriers for consumers who may be resistant to authentication methods they perceive to be challenging, time-consuming, or confusing.

Dynamic Security Policies

Paramount to any risk-based authentication (RBA) scheme is the need to dynamically adjust the level of security required from end users based on the risk of the transaction or service requested. LaunchKey empowers such RBA flows with dynamic security policies that can be attached to individual authorization requests and enforced programmatically.

Next-gen Architecture

LaunchKey was architected with a security-by-design approach consisting of three core architectural characteristics: decentralization, anonymity, and advanced cryptography. These characteristics make the authentication process inherently more secure and mitigate common attacks like credential replay, man-in-the-middle, and phishing.

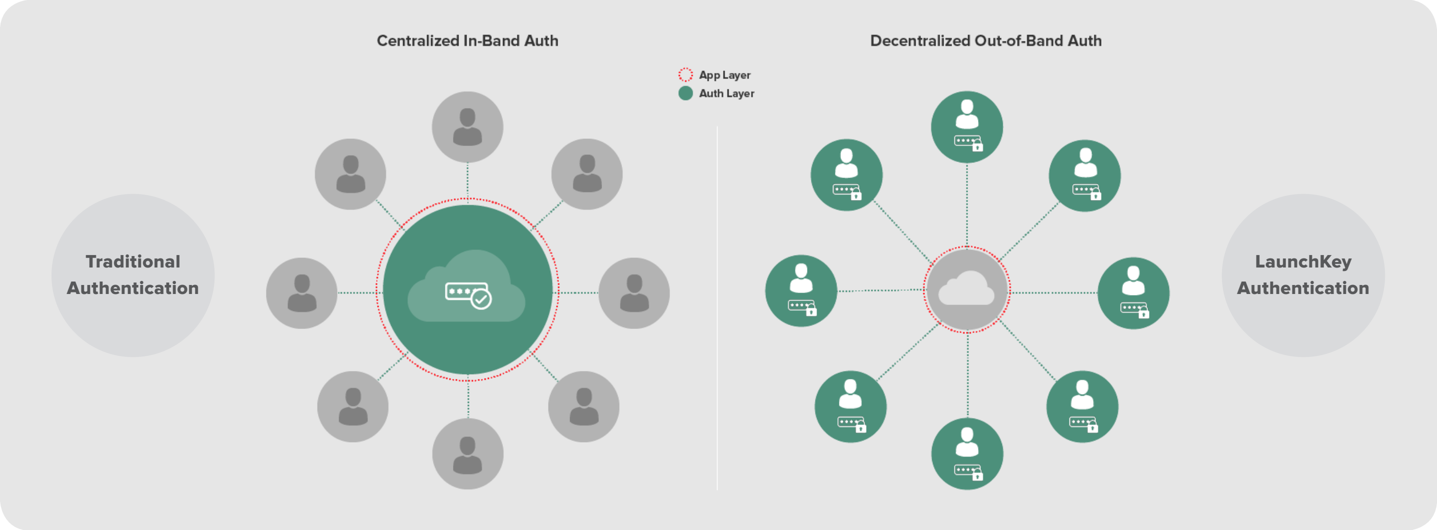
Unlike password-based authentication schemes that involve a vulnerable central repository of credentials, LaunchKey's decentralized approach distributes the layer of authentication to each end user's individual mobile device. Even if an end user's device is compromised, only that user is affected, rather than the entire user base.

All requests and responses that traverse LaunchKey's network are encrypted using public key cryptography. Therefore information LaunchKey processes requires private keys to decrypt, keys that are stored on the end user's device or by the requesting service – not by LaunchKey.

Flexible, White-label Implementations

Central to LaunchKey implementations are two software development kits (SDKs): the Authenticator SDK which enables end users to receive and respond to authentication requests through a native mobile app, and the Service SDK which is used by the backend web service of an application to create those requests. Both use a central REST API hosted by iovation, so LaunchKey can be leveraged by any web service that supports REST. And LaunchKey supports SDKs in every major programming language and framework, so it is platform-agnostic.

Unique to LaunchKey is a mobile authenticator that can be completely white-labeled and embedded within your existing mobile app, or a new standalone authenticator app, ensuring a seamless integration that looks and feels like the mobile app.



Key Advantages

- **Fulfill more use cases** – leverage LaunchKey for account access to any digital platform, authorization of any transactional event, digital access control, delegated access, identity verification, and more.
- **Omni-channel authenticator** – give end-users a single powerful authenticator to use across every touchpoint with the business.
- **White-label authenticators** – keep consumers within your own digital channel by theming and branding authenticators to match your own mobile app.
- **Truly multifactor** – enforce strong authentication through multiple authentication methods available for end users to choose from.
- **Platform-agnostic** – leverage LaunchKey with virtually any online service.
- **Decentralized, anonymous architecture** – eliminate or reduce the most common attack vectors associated with password-based authentication.
- **Advanced public-key cryptography** – iovation doesn't possess the private keys necessary to decrypt requests and responses that cross iovation's network.
- **Dynamic security policies** – programmatically adjust the level of security and assurance required at any given time with custom request rules.
- **FraudForce and ClearKey** – leverage risk insight from iovation FraudForce and ClearKey to implement a full risk-based authentication scheme.

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

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com