AllClear ID

AllClearCrossChannel™ Platform

IN PERSON

PHONE

MOBILE

ONLINE

KIOSK

CrossChannel™
PLATFORM

↓↑

Your
Mobile
App

Platform Capabilities:

- Highly Available and Scalable Modern REST APIs

- SDKs for both iOS and Android smart devices

- Apply a precise level of Authentication every time — single or multi-factor

- Enable Step-up Authentication and your Choice of Factors
  - Knowledge (PIN)
  - Inherence (Finger or Facial biometric)
  - Possession (mobile device)

- The CrossChannel™ Platform eliminates passwords

- Omni-channel experience engages your customers to be known online, on mobile, on the phone, via kiosk or in person

- CrossChannel™ SDK empowers an in-app experience, keeping your customers engaged within your branded environment

- Offered as a security hardened and highly available cloud-hosted SaaS solution

CrossChannel Mobile SDK:

- Easily integrated into any mobile iOS or Android app

- Truly password-less design creates a seamless user experience

- Optional self-protecting client SDK functionality secures app and device integrity

- Captures Risk Factors that enable the Service Provider to make risk-based decisions such as detecting anomalies and halting or redirecting transactions

AllClear CrossChannel™
automation radically reduces the friction
in any customer journey caused by:

AUTHENTICATING
THE CUSTOMER

ACQUIRING
ESIGNATURE

AUTHORIZING
TRANSACTIONS

CONFIRMING
CUSTOMER
LOCATION

Built-In Security Capabilities:

- Short Circuit Front End Attacks
  - Password theft and re-use avoided
  - Social Engineering prevented
- Runtime Application Self-Protection for iOS & Android
  - Obfuscation deters reverse engineering of software
  - Hook Detection/ Prevention
  - Debugger, Jailbreak detections
  - Root cloaking & Tampering
  - SSL & WebView Pinning
- Block Man-in-the-Middle Attacks
  - Application layer end-to-end encryption
  - Mutual TLS
- Multiple Risk Factors available to spot Transaction Anomalies including,
  - Device Type, OS Version
  - Device Manufacturer & Model
  - Device/App Environment
  - GPS Coordinates of the transaction

Optional, Add-On Functionality to Prevent App and Device Attacks

- Device Cloning
- Malware
- SIM Swapping
- App Repackaging
- App Emulation

CrossChannel Platform™: How it Works for Authentication
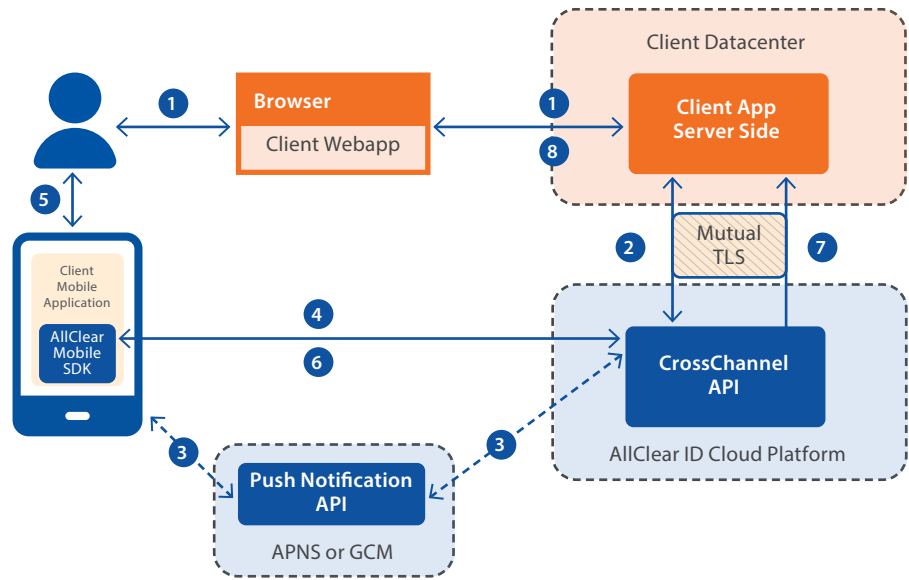
EXAMPLE INTEGRATION

1. Start: Your customer is already an established end-user
2. The end user begins the login process on your website or client facing portal
3. Your back-end calls the CrossChannel API to initiate authentication
4. A push notification is sent to the end-user's mobile device to make your mobile app aware that an authentication is in progress
5. The mobile app fetches the authentication context
6. The AuthN request is presented to the end user who either completes it using the set of factors you require, or declines the request
7. The AuthN request is completed by the mobile app calling back to AllClear ID Mobile Gateway
8. The CrossChannel Service calls back to your back-end with the result of the authentication
9. Your web app retrieves the results of the authentication and displays the appropriate context to the end user

CrossChannel Platform™: More Secure by Design

SHORT CIRCUIT FRONT END ATTACKS

BLOCK MAN-IN-THE-MIDDLE ATTACKS

DETECT AND PREVENT APP ATTACKS

For more information about AllClear ID and AllClear CrossChannel solution

contact: www.allclearid.com or call 1.877.441.3007

AllClear ID