AUTHENTICID

Product Sheet

Smart ReAuth™

Ongoing protection to safeguard consumer and workforce accounts.

Once you have confirmed the person you are doing business with is genuine, preventing unauthorized access and stopping fraud is an ongoing affair. AuthenticID's Smart ReAuth™ leverages facial recognition and liveness detection as a smart choice for additional security with less friction than traditional username/password or two-factor authentication systems. Reduce the risk of compromised accounts or data breaches with a system that doesn't rely on passwords.

What is Smart ReAuth™?

Smart ReAuth™ leverages a selfie image to reauthenticate a user within seconds. During enrollment, the user first goes through a complete identity verification transaction to identify the user as a good actor, with an authenticated identity. Upon consent, an encrypted biometric template is stored with a unique identifier to be used next time an authentication is needed. Going forward, instead of a full identity verification, the user can authenticate instantly, by taking a selfie. Liveness detection and other anti-spoofing checks are performed during the selfie to ensure a person is who they claim to be.

Smart ReAuth™ by AuthenticID offers a biometric-based approach, considered one of the fastest and secure methods available. Smart ReAuth™ provides the highest level of encryption, with one-way hash of images and customizable data storage. When paired with our Fraud Shield™ solution, bad actors who attempt to access your system or data on multiple attempts will be stopped in their tracks.

Here's how Smart ReAuth™ works:

ID is verified at account enrollment through Biometrics

Biometric Authentication (liveness + facematch) is performed and stores encrypted data based on customer requirements.

User forgets password

Link is sent to user via mobile device to reauthenticate.

Customer takes selfie image

Selfie image reauthenticates identity in 5 seconds or less.

Benefits of Smart ReAuth™

Improves the Customer Experience

Smart ReAuth™ can reduce the need for cumbersome processes, like Knowledge-Based Authentication or passwords that can be easily lost, forgotten, or stolen. With AuthenticID's quick, easy selfie capture the user can be verified in less than one second by just looking at their phone.

Reduces Fraud Loss

Smart ReAuth™ enhances security for both businesses and customers. Companies can reduce risk of bad actors committing account theft as well as data breaches, because reauthentication can be triggered by events that could be higher risk: large purchases, account detail changes, or accessing sensitive data. Consumers can avoid identity theft and account takeovers.

Reduces the Demand for IT & Customer Support

Forrester Research indicated in a study that the average cost for an IT department to reset a password is $70. With an automated workflow using Smart ReAuth™, IT departments have a cost-effective and time-savings mode to verify an identity and reauthenticate with minimal effort and maximum security.

$70 Average cost for an IT department to reset a password

Use Cases for Consumers & Employees

Consumers

- Passwordless Logins
- Authorize Purchases
- Authorizing Transfers & Push Payments
- PII-Related Profile Changes
- Changing/Adding Users on Accounts
- Access Account Statements or Sensitive Information
- Unlocking Accounts
- Password Changes
- Lost/Stolen Card Requests
- Turning on Subscription Based Services
- CCPA/GDPR Data Requests
- Authorizing Out-of-Network/Geolocation Logins

Workforce

- Passwordless Logins
- Password Resets & Changes
- Remote & Continued Access to Company Network
- Access to Sensitive Information
- Access to Private Apps
- Biometric Access to Company Facilities
- Unlocking Accounts