appgate

DATA SHEET

AUTHENTICATORS

Choose What's Right for Your Business

All of the factors apply secure authentication across the entire customer population, but when used to complement one another, verification becomes even stronger – without inconveniencing the end user. The solution also offers a single administration point that gives you the ability to change authentication methods over time to adapt to new risks as they arise.

COOKIELESS DEVICE RECOGNITION

The devices used to connect to your firm's transactional webpages are constantly changing: operating system is updated, plug-ins are added or deleted, users change the font size or type, and screen brightness, or clear cookies to free up disk space. This could potentially cause device ID issues, as a device's specifications will not be exactly the same the next time that an end user attempts to log in or make a transaction. But Authentication's device algorithm has the ability to recognize a specific device even when changes have been made, and can also effectively detect new devices.

Taking a heuristic approach, device recognition works by comparing a user's current device to the contextual information previously gathered for known devices and stored in the database. This drastically lowers collision rates, or the chances of a device being confused for a similar one.

MOBILE DEVICE ID SDK

Using a proprietary algorithm, our Mobile Authentication Software Development Kit (SDK) generates a fingerprint for mobile devices based on their hardware and software characteristics, such as the serial, phone, and model numbers. This creates a device id that uniquely identifies mobile devices and is resistant to minor changes, such as if the app is deleted and re-installed. Appgate's SDK allows the device ID to be registered transparently, meaning that there is no change to the end user's experience in the mobile app.

PUSH AUTHENTICATION

With this solution the end user can verify transactions, logins, and any other sensitive requests with a mere push of a button. Customers respond to activity simply by pressing Accept or Reject when prompted. The authentication response is then sent from the user's mobile device to your company's systems via an encrypted communication channel, meaning it is not vulnerable to dangerous Man-in-the-Middle attacks. The solution is made available through our software development kit (SDK) and easily

BENEFITS:

Use the authentication factors that work best for your organization.

Frictionless Authentication for Digital Channels.

Complement your current security solutions and deploy quickly, layering simple and strong authentication on top of your existing infrastructure.

Authentication provides a comprehensive Software Development Kit (SDK) allowing mobile application owners to integrate authentication and electronic signing into their own native mobile apps. Through a complete library of APIs, mobile app owners can extend and strengthen security and deliver unprecedented convenience to end users.

integrates into your organization's native mobile app. The solution is Android and iPhone iOS API supported, allowing for different phones to add fingerprint validation. Fingerprint readers can be combined with Push notifications for strong, layered user authentication.

MOBILE SOFTWARE TOKENS

Authentication can provide software-based one-time passcodes to validate login and transactional activity. It uses the OATH standard for the time-based, single-use passcode, and also supports multiple identities on the same application. In addition, Authentication comes with a robust set of rich APIs that cover an organization's authentication, self-service and administrative needs, and is available on today's leading mobile operating systems, Apple iOS and Android.

BIOMETRIC FACIAL RECOGNITION

Facial Recognition and Liveness Detection from SelfID help combat fraud while still providing an excellent user experience. Using the device's camera, SelfID prompts users to perform gestures such as side-to-side movement in order to authenticate a transaction, thus protecting against fraudsters who may try to circumvent less sophisticated facial scanners with static photos of the end user.

BIOMETRIC VOICE RECOGNITION

Our biometric voice authentication solution employs an end-user's voice as a personalized authentication factor. The software first prompts an end user to record themselves speaking a phrase, which is then registered in our databases. Thereafter, users can authenticate a transaction or login activity by speaking a password or a simple phrase.

EMAIL AND SMS OTPS

Authentication offers out-of-band one-time passcodes (OTPs) through a variety of secure delivery methods, including email or a text message sent directly to the end user's cellphone.

VOICEOTP

With our innovative VoiceOTP feature, end users receive the temporary password via phone call. When the user answers his or her phone, Authentication plays a message that gives a brief introduction and then the randomly-generated passcode, putting the number out of the reach of cybercriminals. The solution is an ideal alternative when data is not available and Push authentication cannot be performed. It also functions when the user is attempting to make a transaction on a laptop or desktop but does not have access to a cellphone.

QR AUTHENTICATION

The QR-code authentication solution is integrated directly into a company's native mobile app, and allows for quick user verification without having to memorize and enter a user name and password. Using a mobile device's camera the encrypted QR code is scanned when an end user wants to confirm or cancel a transaction. Once registered, end users are able to scan the encrypted code generated every time a banking transaction is processed, protecting them from potential fraud attacks. In addittion, the API offers the option to create an even more advanced and customized visualization of the authentication process through QR codes.

OTHER AUTHENTICATION METHODS

Appgate also offers an assortment of specialized authentication factors to suit the unique needs of our clients, including:

- Keyfob Hardware Tokens
- Challenge-Response Hardware Tokens
- Mutual Authentication
- Grid Cards
- Challenge Questions