AUTHENTICATE. COMPLY. DELIGHT.

Wherever you are on your PSD2 Strong Customer Authentication journey, rely on partners that have security and privacy by design.

PSD2, RTS and Biometrics

PSD2 and in particular, Strong Customer Authentication (SCA) divides opinion. Young challengers have open banking in their DNA, more established legacy banks less so.

Whatever your sentiment, SCA has never come at a more appropriate time. As mobile app fraud is up nearly 700% since 2015[1], adherence to PSD2's Regulatory Technical Standards (RTS) ensures protection for all parties, whilst providing the much-needed environment to stimulate and encourage innovation.

[1] RSA Fraud Report, Q1 2018

Under RTS, customer authentication requests need to fulfil three criteria:

1) Protect the confidentiality of the authentication data
2) Ensure that these two are independent from each other and that the breach of one would not compromise the reliability of the other
3) Use two of the three following factors: knowledge, possession, inherence

Biometrics are by their very nature inherent, and AimBrain has built its model around security and confidentiality, to fit with both the demands of PSD2 RTS as well as best practice privacy by design.

AimBrain: Authentication Fit For PSD2 Purpose

The AimBrain server-side authentication model aligns with PSD2's RTS criteria, supporting today's financial institutions through its highly secure, pseudonymised and remote authentication protocol.

ENSURING INTEGRITY, CONFIDENTIALITY AND PROTECTION OF PSCS

(Personalised Security Credentials)

Our suitability for this requirement is demonstrated in two ways:

1 - Our architecture. AimBrain SDKs are integrated within the institution's secure architecture. An authentication request is captured via our SDKs in the FI's web or mobile app, then sent through the FI's secure channels to its infrastructure. Here, the FI stamps the authentication request with a unique randomised ID to pseudonymise the data, before sending to the AimBrain server for authentication against a biometric template. AimBrain returns a JSON file containing the unique ID plus the risk-based score of user authenticity, along with a liveliness and anti-spoof score. Contractually we insist on zero access to PII.

2 - Our data treatment. Biometric templates are stored as algorithmically-derived mathematical constructs on our server. Images or voice recordings are encoded into a new n-dimensional space that represent a highly compressed representation of the original, reducing the image or recording by a factor of x384. This is a lossy information procedure; much of the signal is discarded and only features in distributed representations are encoded. Features of distributed representations of non-linear spaces are highly convoluted, so one feature in the manifold can be interpreted as a combination of it with the rest of the set. Put simply; AimBrain never knows the details or distinctions between data such as faces. Our algorithms know that two faces are different, but do not know in which sense they differ. This protects against image or voice reconstruction, since each representation captures a different element for each request.

aimbrain
simply smarter authentication

AimBrain - PSD2 RTS

INDEPENDENCE OF CHANNELS

PSD2 requires that the channel for initiating a payment or action is independent of the channel from which the authentication code is received. AimBrain provides a safe, independent channel that - if breached - would contain neither personally identifiable data nor raw biometric data. We protect against the possibility of a single vector attack through our location in the cloud. In order to breach a transaction, fraudsters would need to have intercepted the device request, the bank's unique identifier and AimBrain's pseudonymised response; the unlikelihood of which makes our remote authentication model a more obvious security choice.

UNDERIVABLE AUTHENTICATION CODES

Under PSD2's RTS, authentication codes must not give any indication about the other authentication elements and mechanisms, nor allow for the derivation or forgery of a new code from a previous version. The AimBrain authentication process uses biometrics instead of tokens, which are protected by market-leading anti-spoof and liveliness detection to prevent against identity fraud. Randomised challenges and combinations of biometrics such as facial, audio and lip movement provide an impenetrable barrier against spoofing attacks.

AIMBRAIN TECHNOLOGY

The **AimBrain** server-side authentication suite is available as individual components or as bundles, each of which is deployed via SDKs using open APIs (TLS and HMAC-secured). We integrate directly into the enterprise's application using the enterprise's secure channel, and provide a risk-based score in industry standard JSON format, for easy consumption for downstream systems.

PRIVACY BY DESIGN

AimBrain *is a security company and commits to the highest levels of data privacy and security. AimBrain insists on a zero-access agreement to an organisation's sensitive data. Extensive testing has proven that our data cannot be reverse-engineered, and can be rendered useless in the event of any suspected breach.*

For more information or to discuss stronger user authentication under PSD2, email sales@aimbrain.com.