Biometrics & 2 factor authentication

ABSTRACT

Bank customers are looking for a friction-free experience across all channels. This whitepaper examines the use of OTPs and what alternatives are available for banks looking to maintain high security, comply with regulation but also increase ease of use.

There isn't a bank in the world that's not considering biometrics as a way of combating fraud, complying with regulations or improving the customer journey. It's worth taking a step back and considering why this is the case and looking at some of the benefits. Let's start by examining a particular use case and explaining how biometrics will improve things and why they are needed.

Let's explore a use case that is very typical today when a bank customer wants to carry out a simple task while using internet or mobile banking, such as adding a new payee, making a transaction over a certain size or changing personal details (e.g. change of an address).

At this point, a standard way to authenticate the user is to send a One Time Password (OTP) via SMS or an e-mail to the user (using the details the bank have on record) so that he or she can enter this into the internet or mobile banking portal to 'close the loop' and the bank can confirm identity. These are called software tokens. Simple right? Well no. There are some big problems that this whitepaper will look into.

Firstly, soft tokens are not safe. They can be duplicated and, because they are something one doesn't physically possess, they are exposed to unique threats based on duplication of the underlying cryptographic material - for example, computer viruses and software attacks. They can also be subject to 'man in the middle' attacks before reaching the intended user.

Added to this, many customers don't like them as they add too much friction into a process that they want to be friction free. There is a general consensus that, once being allowed in, a customer should be able to do what they like and the OTP request adds an unwanted step - especially when the device isn't at hand (such as trying to make an internet payment when you don't have your phone that's just about to receive an SMS OTP).

This leads to another big global issue our clients see. In many countries OTPs fail to arrive. This can be down to unreliable cellular coverage or simply people traveling internationally and not receiving the required SMS (such as a person with a UAE local bank's mobile application, trying to make a payment when in, for example, Africa). This is an important demographic for mobile and internet banking and, according to www.itproportal.com, industry sources suggest that as many as 13 per cent of OTPs sent as part of a 2FA-secured transaction might never be received. It's not just an SMS issue, e-mails can be delayed (or lost in spam) for longer than the bank allows them to be active.

If the security threat, the fact that they are not liked by customers and sometimes won't arrive (leading to a loss of both revenue and customer confidence) isn't enough, there is global regulation coming up that could be the final nail in the OTP coffin. A good example is the strong customer authentication part of PSD2 expected to be finalised soon that makes it quite clear that SMS-based authentication will have a hard time meeting the requirements, especially those related to approving payments (in August 2016, the European Banking Authority (EBA) published its draft proposal for the Regulatory Technical Standard (RTS) on Strong Customer Authentication (SCA))

Some banks have attempted to deal with the issue by providing hard tokens as an alternative. This is where the credentials are stored on a dedicated hardware device and therefore cannot be duplicated (absent of a physical invasion of the device) however these have their own, and similar, problems. Who in today's fast moving connected world wants to carry a bank-dedicated device to make a payment (or, as is more likely the case, wait until they get home to make a payment)? Consider also that hard tokens are even more expensive than soft tokens, need maintenance (batteries) and are not practical in many regions (how do you send one to a customer in a country that doesn't have an effective postal or address system - as is the case in some of the biggest mobile banking markets such as Africa, Asia and the Middle East).

There is also increasing fraud reported that include bot-based ‘man-in-the-middle’ or simple phishing attacks. These are aimed at both hard and soft tokens in which the one time password provided by the token is solicited, and then supplied to the genuine website in a timely manner.

So what can biometrics do to help? Are there other options?

Firstly, we need to look at what’s acceptable for multi-factor authentication. It’s well defined as two or more independent credentials that are categorised as knowledge, possession and inherence.

Knowledge: *something only a user will know such as a PIN / Password*
Possession: *something only a user possesses such as a soft or hard token*
Inherence: *something that only a user is such as a biometric*

Biometrics allow a bank to turn the actual banking app into the authentication device by implementing Inherence. Let's examine this and it’s practicality - first looking at a single biometric and then a combination

The strongest biometric on a mobile or internet banking portal will always be behavioural authentication whereby the mobile banking application or website can, with high accuracy, confirm the authentication of a user by the way he or she uses the device (not what they do, how they do it). Why do we think it's the strongest? Firstly because it’s a passive authentication methodology (your users, and thus potential fraudsters, don’t know it's there or even that they have been learnt) and, secondly, because of very recent developments in the application of deep learning techniques one can achieve previously unseen accuracy.

So how could it work?

Step 1: a bank needs to run behavioural analysis in ‘listen only’ for a number of months. This will allow the bank to learn it’s customers behaviour and understand how behavioural authentication can be implemented. Key factors a bank should be looking for when doing this analysis are:

- What percentage of our users can be authenticated using behavioural authentication?
- How many ‘usage sessions’ does it take to learn (enroll) someone?
- What range of behavioural scores can we achieve?
- How can we use these scores to determine when someone is who they say they are?
- When do we know someone certainly isn't who they say they are?
- What scores should we be looking for, for certain transaction types and how how can we use this for extra security (‘step up’)?

Step 2: once you have the data you can use the benchmark scores to illustrate how you can implement behavioural authentication. Let’s assume the following:

- At 87% you are happy that to accept the person is who they say they are;
- Below 75% you would require further authentication before making that decision;
- Scores were as high as 98% at times and the majority of scores range between 87 - 98%.

Step 3: implement a process which allows a customer with a behavioural score of over 87% to carry out a transaction without being sent an OTP. Remember that this complies with multi-factor authentication as the customer entered the mobile banking app with a password (t*ick knowledge*) and was behaviourally authenticated to above 87% (*tick inherence*). Continuing down the stronger authentication route, a bank can increase the required behavioural threshold for more highly sensitive transactions. Maybe a payment of, for example, GBP 500 would need a score of 97%.

But what happens if the customer doesn't have the required score? At that time the bank could elect to send an OTP (drastically cutting down the number that need to be sent). We work with a number of banks that start looking at the typical 80/20 rule and aiming to see if 80% of their mobile or internet banking traffic can be authenticated without needing to send an OTP.

While this is good, we would argue that biometrics can have a further application in this use case. Why not ‘step up’ to another type of biometric if the customer fails to achieve the correct behavioural score? Consider this as an example. When a customer of a bank that’s using behavioural authentication fails to achieve the correct behavioural score, why not then use facial authentication to compare the user and the KYC documentation that the bank already has? The bank could then use the combined score to authenticate the customer successfully.

This is a good interjection into one of the key themes we see with biometric authentication in banks. While there is a lot of focus around security, fraud prevention and regulation, the real focus should be around the customer journey. Not just how biometrics will enable a wider range of products and services to be offered to a customer in the channel they want, but looking at the customer journey across the bank. Customers move between channels, one day transacting at home using mobile and internet banking, then the next day on the phone, the next day in branch

and the next day via the ATM. There has to be consistency of the authentication strategy. Why register someone for facial authentication on a mobile app but then ask for ID in a branch? Why not make sure the person withdrawing money from an ATM is indeed who they say they are? Why implement expensive voice authentication technology and limit it to a single channel? That's not what your customers want.

As a last observation we need to take a step back and look at the smart phone and how it can be used as the authentication device across any channel. When authentication became a key focus over 10 years ago, banks couldn't really explore how the smartphone could be used instead of a token as they were not yet everywhere. However times have changed and this has become a reality, indeed a necessity. Looking at the customer journey, why not provide your customers with a way to authenticate on the device they never leave the house without. This is something we work with banks on every day.

About AimBrain

AimBrain, a next-generation biometrics engineering company, helps financial institutions easily, securely, and accurately authenticate their users across any channel. Using a patent-pending, context-based step-up authentication methodology, AimBrain is helping some of the world's largest financial institutions know if their users are really who they say they are.

AimBrain delivers advanced biometrics technology to banks so they can stay ahead of mobile fraud through a secure and frictionless authentication experience. Supported by Episode1, a leading UK venture capitalist, AimBrain is largely recognised for their potential to revolutionise the world of money and has been named as a 2016 FinTech50 finalist.