typingdna

Typing Biometrics Authentication

Choosing the Right Authenticator for PSD2 SCA

Contents

Summary

The pressure placed on financial institutions keeps increasing due to challenger banks and evolving regulation demands, including PSD2, and GDPR. There are huge potential financial penalties for failing to meet every regulation.

At the same time, security demands can be at odds with the user experience. This means that a viable trade-off must be found between the demands of regulators and the needs of the average user. Hence, a comprehensive framework that every financial institution should use to evaluate authenticators is introduced.

As an inherence-based authenticator, typing biometrics running on usernames and passwords are presented as an alternative that drives the needed security without burdening the user experience.

Regulation Overview

There is an enormous amount of pressure placed on financial institutions to keep growing while simultaneously adhering to constantly evolving regulatory guidelines. Experts estimate that some banks spend as much as $4 billion annually on regulations adherence alone, which understandably makes high level executives and investors nervous.

When you add the need to compete with challenger banks into the mix, it becomes extremely difficult for well-established financial institutions to remain fully compliant without overspending or sacrificing the quality experience their customers expect. Fortunately, new fintech companies help relieve some of this burden, thereby making it possible for banks to improve the user experience and stay on top of all regulations.

PSD2 demands Strong Customer Authentication

The second Payment Services Directive (PSD2) establishes new payment options for consumers by giving merchants the ability to acquire customer data directly from their bank. Along with this, PSD2 requires enhanced identity checks for online payments. All of this has been in motion since 2015, but it won't be finalized until 2018. Despite this, banks in the EU have already been making the anticipated necessary changes in order to avoid a last-minute crunch.

Strong Customer Authentication (SCA, defined by article 4, paragraph 30, PSD2 EU - Directive 2015/2366) is one of the primary points that financial institutions need to address under PSD2. There are three SCA options to choose from: knowledge (something only the user knows: password, PIN), possession (something only the user possesses: token, mobile), and inherence (something the user is: typing biometrics, fingerprint).

Every applicable company must use at least two of the three in most transactions or operations involving Account Information Service Providers, Payment Initiation Service Providers and Account Servicing Payment Service Providers.

Several SCA technical compliance requirements must be utilized. For example, all financial services companies are responsible for implementing measures that will drastically reduce the risk of inherence based SCA such as behavioral biometrics being uncoverable by an unauthorized party. It's also necessary for financial services companies to mitigate the risks involved in using multipurpose devices, including smartphones and tablets.

GDPR emphasizes the importance of security compliance

The General Data Protection Regulation (GDPR) goes into full effect on May 25, 2018. GDPR guidelines require any business based in the EU, processing data in the EU or selling to customers in the EU to take proactive measures that will keep consumer data safe. For instance, if a US based company sells products to anyone in any of the EU countries, they have to be compliant with the GDPR. Failure to follow the GDPR could cause the offending company to pay a fine worth up to 4 percent of their annual group revenue.

Any data breach is instantly viewed as a failure to comply with the GDPR. In other words, companies that don't ensure SCA is properly in place could be hit with a massive fine if a breach happens. Therefore, businesses that fully follow PSD2 regulations will be in a good position to also be in compliance with GDPR.

Although setting all of this up may seem daunting and costly, the reality is that keeping consumer data safe is one of the best ways to maintain a good business reputation.

Choosing the right authenticator in terms of security and user experience

Compliance is just your first step. In other words, choosing two of the three approved SCA methods (inherence, possession and knowledge). Each SCA you select must be independent and not rely solely on one device that could become compromised.

Comparing the security of authenticators needs a solid framework

Next comes security measures, which are broken up into three distinct parts via the Strength of Function for Authenticators (SOFA) framework.

1. Baseline Conditions – All data exchange protocols must be secured at all times; data storage needs redundancy; data must be encrypted and run through secured connections.

2. Accuracy – How likely is each SCA method to be accessed by the wrong person? Authenticator accuracy determines how well each authenticator recognizes true and false attempts that hackers use to try to trick their way into an account. High quality SCA methods deliver a good accuracy rate without requiring human intervention.

3. Resilience – Going along with accuracy, how easy is it for someone to hack, spoof, socially engineer or phish their way into a user's account? An SCA with low resilience could be targeted by cybercriminals. High resiliency makes it much more difficult for attackers to trick the algorithm into confusing false SCA with a positive result. For instance, passwords are extremely vulnerable due to low resilience, but typing biometrics aren't. Between accuracy and resilience, typing biometrics are well-positioned to offer a high quality SCA for financial institutions.

User experience can easily become the victim of SCA

There are numerous SCA methods a business can implement, but it's critical to carefully consider the user experience. For instance, when VISA began using 3D Secure with SMS in Brazil, it made conversion rates drop by a staggering 55 percent. This highlights the fact that becoming compliant is easy, but the hard part is simultaneously taking a smart approach that delivers good UX.

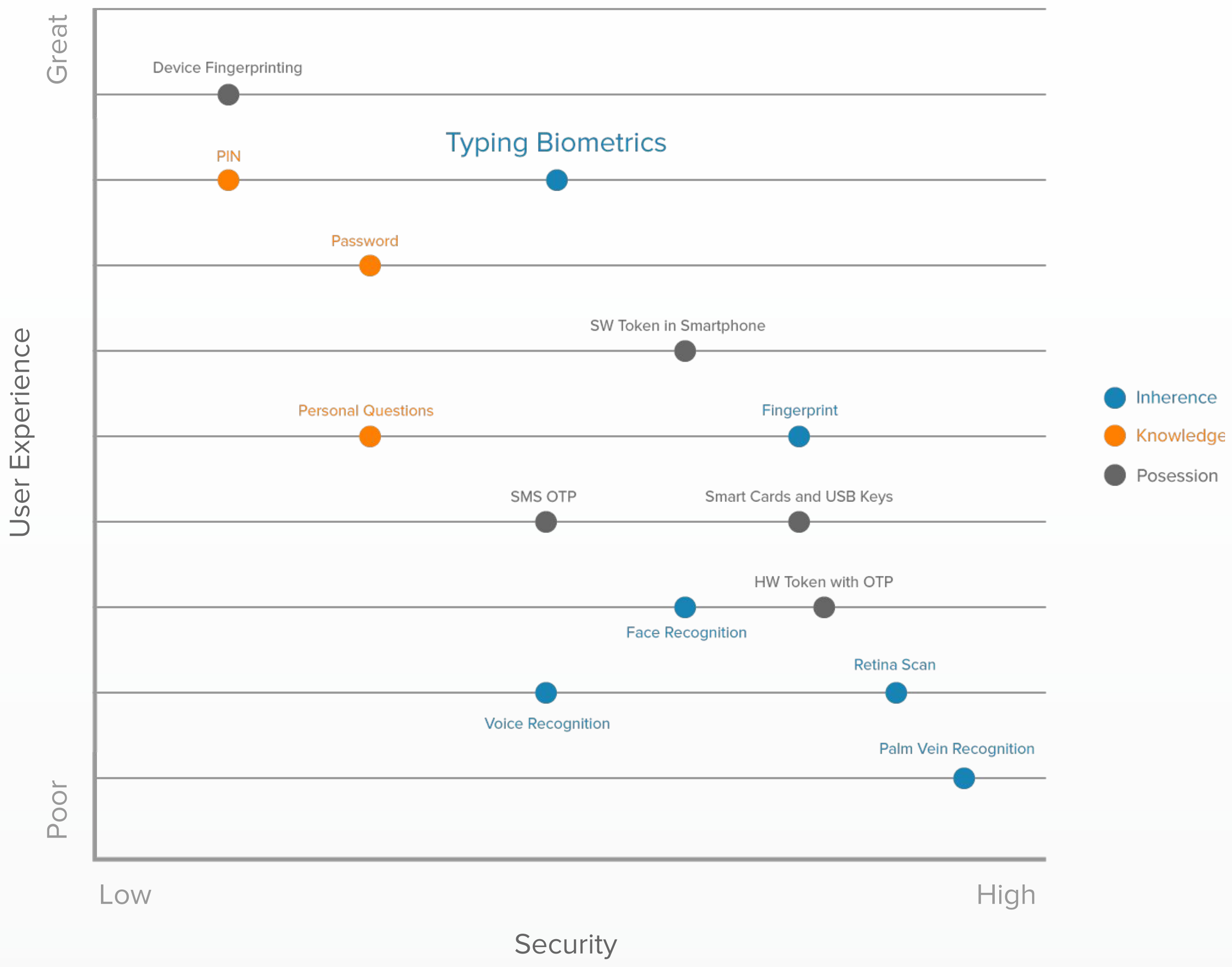
To make matters worse, consumers are constantly becoming more demanding of their apps and other software. Therefore, if organizations don't use frictionless authentication methods, they are going to lose a large portion of their customer base.

The sad truth is that every company that fails to properly consider the user experience is currently being outdone by a competitor that can entice consumers away with a faster, more streamlined process.

Keeping the right balance between security and user experience is essential

The chart below offers a non-exhaustive overview of authenticators and is compiled via a general industry consensus about the relative position of each authenticator versus every other authenticator. The implementation of each authenticator can greatly affect security and user experience. Please note that this example isn't meant to give conclusive answers regarding which authentication methods are best for financial institutions, but it can provide a baseline for determining how to move forward with SCA compliance.

Comparing Authentication Methods



By reviewing the chart, we can find a few patterns of interest.

- There is often a trade-off between security and user-experience.
- Knowledge based factors are very user friendly, especially because users are already used to them, but they tend to not be very secure.
- Possession factors are safer than knowledge, but they're not as user-friendly because items such as smartphones can be lost.
- Biometrics are usually the safest option. However, they can also require a lot of user involvement, leading to poor user experience.

Any company attempting to determine which SCA methods are best for their specific situation should consider plotting their potential authenticators in a similar manner to make the most informed decision.

Typing Biometrics Authentication

One SCA method, inherence, relies on the behavior of each user. Meanwhile, knowledge requires the user to provide something they know such as a PIN or password. Possession works when users have a certain item with them such as a smartphone.
Behavioral biometrics is a field that's dedicated to inherence. In a nutshell, it means that the SCA system learns a certain behavior that's exhibited by each user such as gait, voice or typing style. From there, the system is able to easily recognize whether or not the correct person is accessing each account.

A great balance between security and user experience

Typing biometrics are an SCA option that offers a no-compromise solution between security and user-experience. Accounts are secured via an artificial intelligence based algorithms that analyzes typing patterns to accurately identify users. The best part is that this is something that doesn't have to take a lot of time, and it is performed in the background. After all, web users spend most of their online time typing, and they all have their own unique typing pattern. For example, some people hunt and peck on their keyboard, but others fly across the keys so quickly that it barely seems possible. Each user also has certain words or characters that they always pause before typing. Typing biometrics take all these factors into account to deliver a top-notch SCA method.

A passive method of typing biometrics checks a user's typing pattern when they enter their username and password or card number and cardholder's name. With TypingDNA, in 80 percent of cases, this is enough to instantly clear valid users beyond the shadow of a doubt (FAR of approximately 0.1 percent).

The remaining instances will lead to a secondary form of authentication becoming required. This enables websites to adhere to PSD2 regulations without harming the user experience.

Behaviour-based authentication delivers great resilience against mimicking

It's practically impossible to mimic someone's typing patterns, which makes typing biometrics extremely difficult to spoof. Further, accuracy testing has indicated typing biometrics can provide a false acceptance rate (FAR) as low as 0.15 percent. Enhanced security measures boost customer confidence, including the fact that typing biometrics doesn't store the typed text and uses the latest encryption techniques and secure connections for transfer and storage.

Invisible authentication keeps the user experience intact

Most users will never even need to think about typing biometrics, especially after their account security measures are initially set up. This is because 80 percent of users will be cleared in the background by completing tasks they're already required to do such as providing their username and password. Moreover, typing biometrics from TypingDNA deliver a consistent experience for users, regardless of which device they use.

In fact, the solution works the same for desktops and smartphones, and it also keeps delivering the same high level of accuracy if the user changes keyboards. All-in-all, this passive approach enhances security without aggravating users.

No hardware means low TCO

Most inherence based SCAs require the user to have some type of equipment. For example, if you wanted to observe their gatit, they'd have to use accelerometers. Some SCAs also rely on techniques such as facial recognition or a fingerprint scan. Not only are these methods more obtrusive for users but they require investing in the technology. With typing biometrics, organizations can get authentication that has a much lower total cost of ownership (TCO) and doesn't ask users to do anything other than use their computer or smartphone's existing keyboard.

Organizations want to be up and running quickly…

Financial institutions and other businesses can easily plug TypingDNA into their existing legacy systems via a RESTful API. The program is made to be deployable on-site or in the cloud. Most companies will be up and running in less than one month.

…and deliver the same experience across devices

One of the main points for user experience is whether or not the interface is simple to use. Typing biometrics from TypingDNA deliver a consistent experience for users, regardless of which device they use. In fact, this SCA works the same for desktops and smartphones, and it also keeps delivering the same high level of accuracy if the user changes keyboards.

Conclusion

The pressure placed on financial institutions keeps increasing due to challenger banks and evolving regulation demands, including PSD2, and GDPR. There are huge potential financial penalties for failing to meet every regulation.

At the same time, security demands can be at odds with the user experience. This means that a viable trade-off must be found between the demands of regulators and the needs of the average user.

The actual security of each authenticator is based primarily on two factors: accuracy and how easy it is to bypass. Something as simple as a password is often easily bypassed because hackers can easily get this data. Meanwhile, typing biometrics are much more secure because it's practically impossible to steal someone's exact typing pattern and be able to emulate it on command.

Financial institutions must use at least two of the three recommended SCA categories: inherence, possession and knowledge. There are several options available in each category, and they all have varying levels of security versus user experience. For example, typing in a username and password is very easy for users, even though it's long been established that it's not truly secure. Combine this with a backup SCA such as typing biometrics, though, and suddenly each user's account becomes a lot safer.

Ultimately, typing biometrics is a way to improve security and be compliant with PSD2 regulations without having a notable impact on the user experience. The reality is that most users will never even encounter a third SCA when typing biometrics are in play, meaning that the entire thing will be just as fast and smooth as it currently is to enter nothing more than a username and password.

However, this outdated approach becomes viable and truly secure again because of the work that typing biometrics does in the background.

About TypingDNA

TypingDNA is a cyber security SaaS company which develops proprietary AI-based behavioral biometrics technology. We focus on typing biometrics (a.k.a. keystroke dynamics), identifying users based on how they use their keyboards. Flight and dwell times (the time needed to find a key and the time needed to press a key) measured for a text that is only a few characters long is enough for us to do real-time authentications.

TypingDNA's typing biometrics allow businesses and their users to be protected against account take-overs and online fraud without burdening the user experience. Our partners are rewriting the rules of the game, using innovation to be one step ahead of attackers instead of bracing for the worst.

Try our quick online demo

See typing biometric authentication at work for
username and password, and online credit card payments scenarios.

Contact our team

✉ contact@typingdna.com

🖥 typingdna.com

📍 Str. Vasile Conta nr.32, 410320, Oradea, Romania, EU