typingdna

The hard truth about

Running Keystroke Dynamics for PSD2 SCA compliance in 3D-Secure transactions

Using keystroke dynamics to achieve PSD2 SCA compliance is a great solution. This whitepaper provides an overview of why that is and helps clarify three myths that can pose challenges along the way:

Myth 1
Running keystroke dynamics on the OTP entry field is compliant.

Myth 2
Adding keystroke dynamics to the process is enough.

Myth 3
Layering keystroke dynamics with circumstantial evidence ensures compliance.

Some background on PSD2

PSD2, more formally The EU Directive 2015/2366 of the European Parliament and of the Council, was introduced in 2015. However, the most important aspects of it come into force between September 2019 and September 2021. It includes 112 articles and 11 mandates that are examined by the European Banking Association.

The regulation impacts all players in the financial sector from payment providers to banks and beyond. It also encourages competition, transparency, and innovation in the payment services field. PSD2 affects EU consumer access to banking data in many ways. At its core, the provision mandates an open banking approach and higher security through new authentication methods and dynamic linking.

SCA in PSD2

Strong Customer Authentication (SCA) is required for all payer- initiated transactions when both the card issuer and acquirer are within the European Economic Area (EEA). More specifically, it requires at least two independent authentication factors to be used when a payment service user (PSU):

- accesses its online payment account
- initiates an electronic payment
- carries other risky transactions via remote channels

The June 2019 opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 has brought forth much-needed clarifications to compliant authentication methods for both payment service providers (PSPs) and PSUs, including merchants.

The EBA clarifies what constitutes a compliant element in each of the three possible categories of multi-factor authentication: inherence, possession, and knowledge, as per the table below (which is not exhaustive):

Knowledge	**Possession**	**Inherence**
Password	Device confirmed by OTP	Fingerprint
PIN	Device confirmed by signature	Voice recognition
Challenge question	Card or device confirmed by QR Code	Vein recognition
Passphrase	App or browser confirmed via device binding	Hand and face geometry
Swiping path	Card confirmed via card reader	Retina and iris scanning
	Card confirmed via dynamic CVC	Keystroke dynamics
		Heart rate
		Angle at which device is held

To sum it all up, most payment service users within the EEA will need to be authenticated with two independent methods whenever they try to **access their accounts** or **make online payments**.

The easy part: access to and initiation of payments from the online payment account

PSPs usually have direct access to the "online payment account" — in most cases an online or mobile banking platform — making it easy to deploy authentication factors like SMS OTP (despite the increasing security concerns), mobile tokens (unlocked with pins or biometrics) and even hardware tokens (despite their cumbersome maintenance and high cost).

Moreover, in many countries in the EEA, similar authentication standards were enforced by national supervisory authorities before PSD2 came into effect.

The hard part: initiation of electronic payments in online commerce

Electronic payments within the EU are traditionally secured within the 3D-Secure protocol by sending an SMS one-time password (OTP) to the PSU, which is then confirmed. Given the EBA's June 2019 opinion on what can constitute a valid SCA factor, this option was ruled out (as the data printed on the card cannot be considered a knowledge-based element). This required issuers to find a way to add an authentication factor in a very short time, in an economically sensible way, and without harming the user experience (and implicitly the conversion rate).

This is a challenge in itself, and clearly asks for an innovative solution if passwords are to be avoided.

To make things even more complicated, an "electronic payment" involves multiple parties, and no single party holds full control over the PSU's journey. Starting from merchant, acquirer, payment gateway, access control server, and issuer all the way to the credit card network, each party controls or influences the process.

Fortunately, a large number of PSUs do have access to mobile applications provided by issuers. Such applications can be configured to help satisfy SCA compliance requirements by having the PSU confirm their identity via the application (e.g., by providing a fingerprint scan or a PIN). While this still prompts the users for more steps than before, it is a viable option for many, and helps move away from SMS OTPs, as well as their vulnerabilities and costs.

On the other hand, PSUs who do not have access to mobile applications from the issuers need a solution for authorizing electronic payments. Is there a better alternative to passwords?

Keystroke dynamics: A potential solution

After the EBA's June 2019 Opinion on acceptable SCA factors, keystroke dynamics started gaining a lot of traction as an accepted technology. Keystroke dynamics (or typing biometrics) works by recording the time a user spends on specific keys and the time the user needs to find specific keys, all in milliseconds. After that data is captured, the technology compares the samples to previously enrolled typing behavior belonging to each individual user.

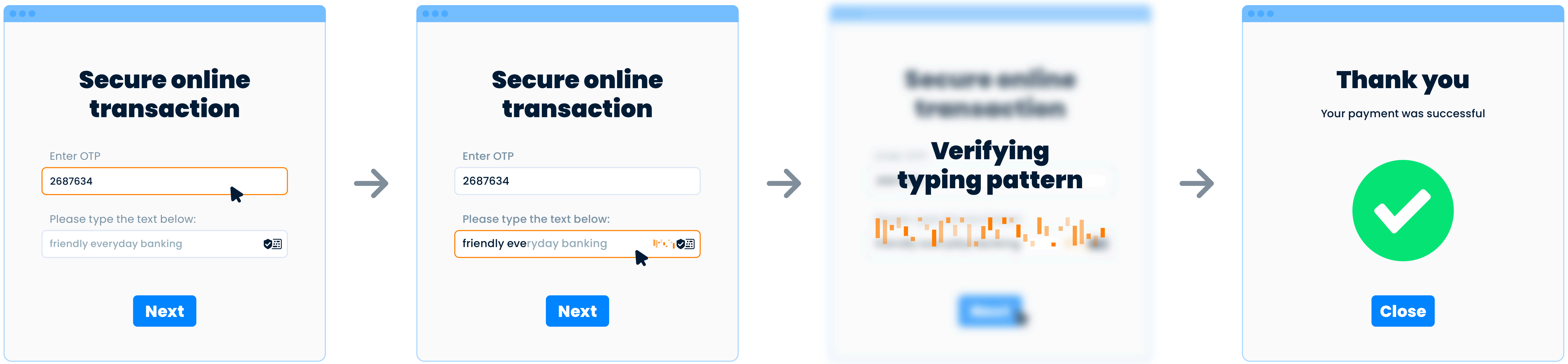
Given the conceptual simplicity and the great user experience of the solution, many important players are adding keystroke dynamics on the entry field for the aforementioned SMS OTP code that is already a traditional part of the 3D-S protocol.

This does seem like a good idea — at first. The three myths that need to be debunked for a successful implementation are:

Myth 1

Running keystroke dynamics on the OTP is compliant

The EBA specifies that the authentication factor should have a "very low probability of an unauthorized party being authenticated as the payer."


Secure online transaction
Enter OTP
2687634
Please type the text below:
friendly everyday banking
Next
Secure online transaction
Enter OTP
2687634
Please type the text below:
friendly everyday banking
Next
Verifying typing pattern
Thank you
Your payment was successful
Close

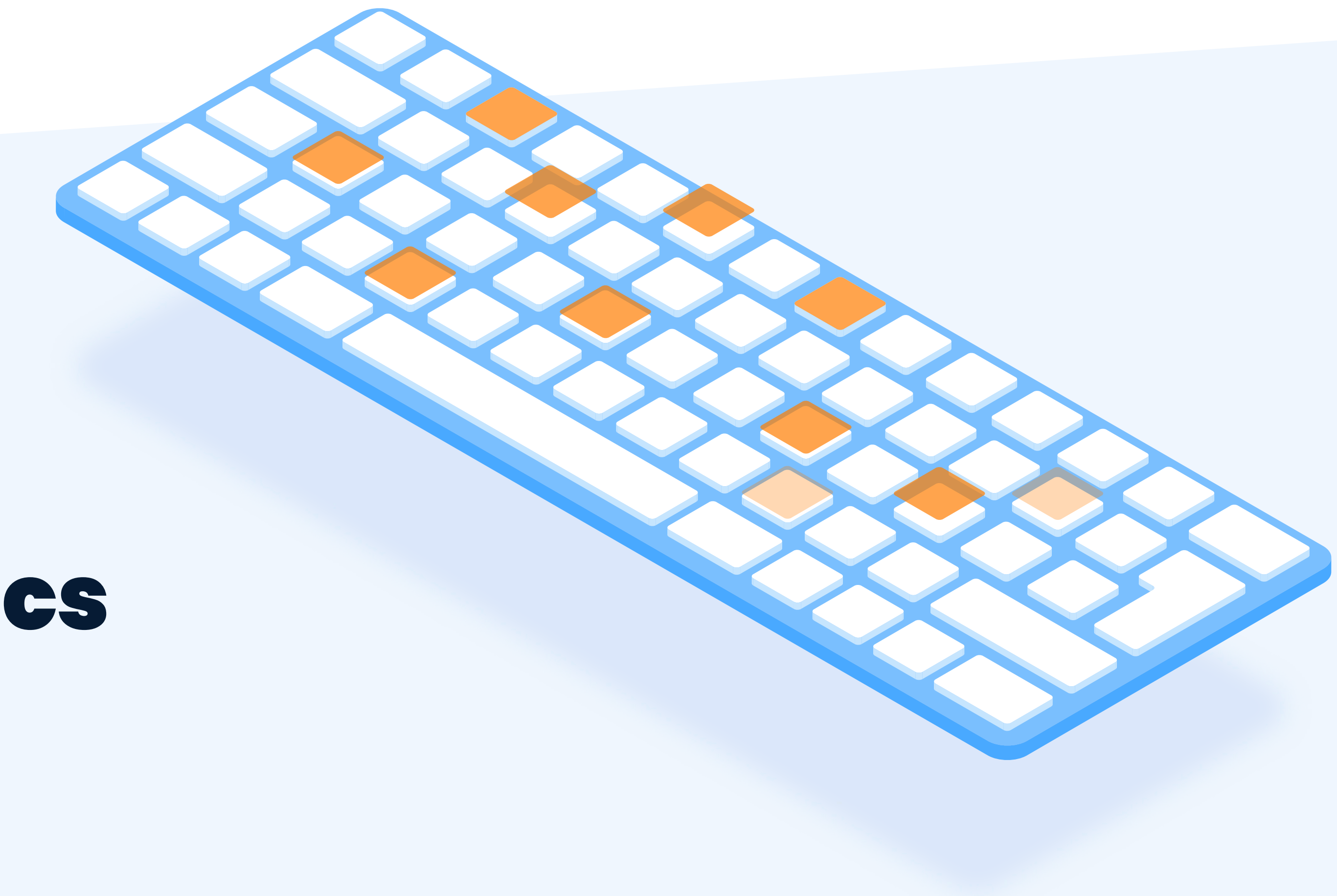
To achieve high accuracy (95%+), keystroke dynamics either use short, repetitive inputs (i.e., 10-30 characters, the same characters each time), or they use long, non-repetitive inputs (i.e., 100+ characters, which can be different every time).

> *Running on an OTP input of 6 to 8 non-repetitive numerical characters will result in accuracy closer to a flip of a coin than to the 95%+ that would be pertinent for online transactions.*
>
> **Raul Popa | Data Scientist | CEO**

In other words, recording how a user types “732 453” tells very little about how the same user will type “549 857” in the future. In order to slightly increase the accuracy, gathering very many samples (i.e., at least 30 samples) can help.

But building up a profile would take a very long long time, risking non- compliance with the current deadlines.

Possible solution: adding a field where the customer can type a short, repetitive string of 10 to 30 characters in order to quickly get to high accuracy and ensure SCA compliance.



Myth 2

Adding keystroke dynamics to the process is enough

Like all biometrics, keystroke dynamics are probabilistic in nature and subject to environmental and physical changes regarding the user.

For example, the same user will provide incomparable typing patterns in the following scenarios: typing on a mobile device in portrait mode, typing on a mobile device in landscape mode, typing on a desktop device, and typing on anything with an injury to a finger.

The logical consequence is that a fail-safe needs to be added for the cases when the user is not recognized (resulting in a false rejection). The False Rejection Rate (FRR) for keystroke dynamics can range from below 1% to 30%, depending on the implementation.

Possible solution: ensuring that the keystroke dynamics implementation is solid so that the FRR is minimized, and implementing a fail-safe to make sure the rightful user can complete the transaction under all circumstances.

Myth 3

Layering keystroke dynamics with circumstantial evidence ensures compliance

Many issuers have access to a plethora of circumstantial evidence around every transaction, ranging from transaction history to location data and light device fingerprinting. Naturally, the use of this data along with keystroke dynamics significantly reduces the probability of an unauthorized party being authenticated as the payer.

However, as per PSD2 SCA, the authentication factor itself (in this case keystroke dynamics) needs to comply with the requirements. Transaction history and other circumstantial data might provide an exemption for SCA but will not support compliance.

Possible solution: ensuring that the false acceptance rate (FAR) for the keystroke dynamics solution itself delivers SCA compliance by ensuring a very low probability of an unauthorized party being authenticated as the payer.

Summing it all up

Card issuers in the EU need to ensure that card users are able to perform online transactions as per PSD2 SCA, mostly within the 3D-Secure protocol already in place. PSUs who have access to mobile token applications can be covered more easily, even if the device switching during the transaction remains a problem.

On the other hand, PSUs who do not have access to such applications need to be covered using a different method. Keystroke dynamics is a viable and user-friendly solution, as long as a fail-safe is made available and the accuracy limitations around running on the card holder's OTP input are fully understood.

About TypingDNA

TypingDNA is a behavioral biometrics company based out of New York City. We specialize in providing keystroke dynamics technology (also known as typing biometrics) in order to recognize users based on the way they type.

This AI-based technology makes it easier to prevent fraudulent activity, such as account takeovers, in a non-obtrusive way that doesn’t require any special equipment.

TypingDNA works with financial, retail, and educational organizations around the world, and is backed by VCs like Gradient Ventures (Google’s AI Venture Fund) and Techstars.

✉ contact@typingdna.com

🖥 typingdna.com

@typingdna

@typingdna

typingdna