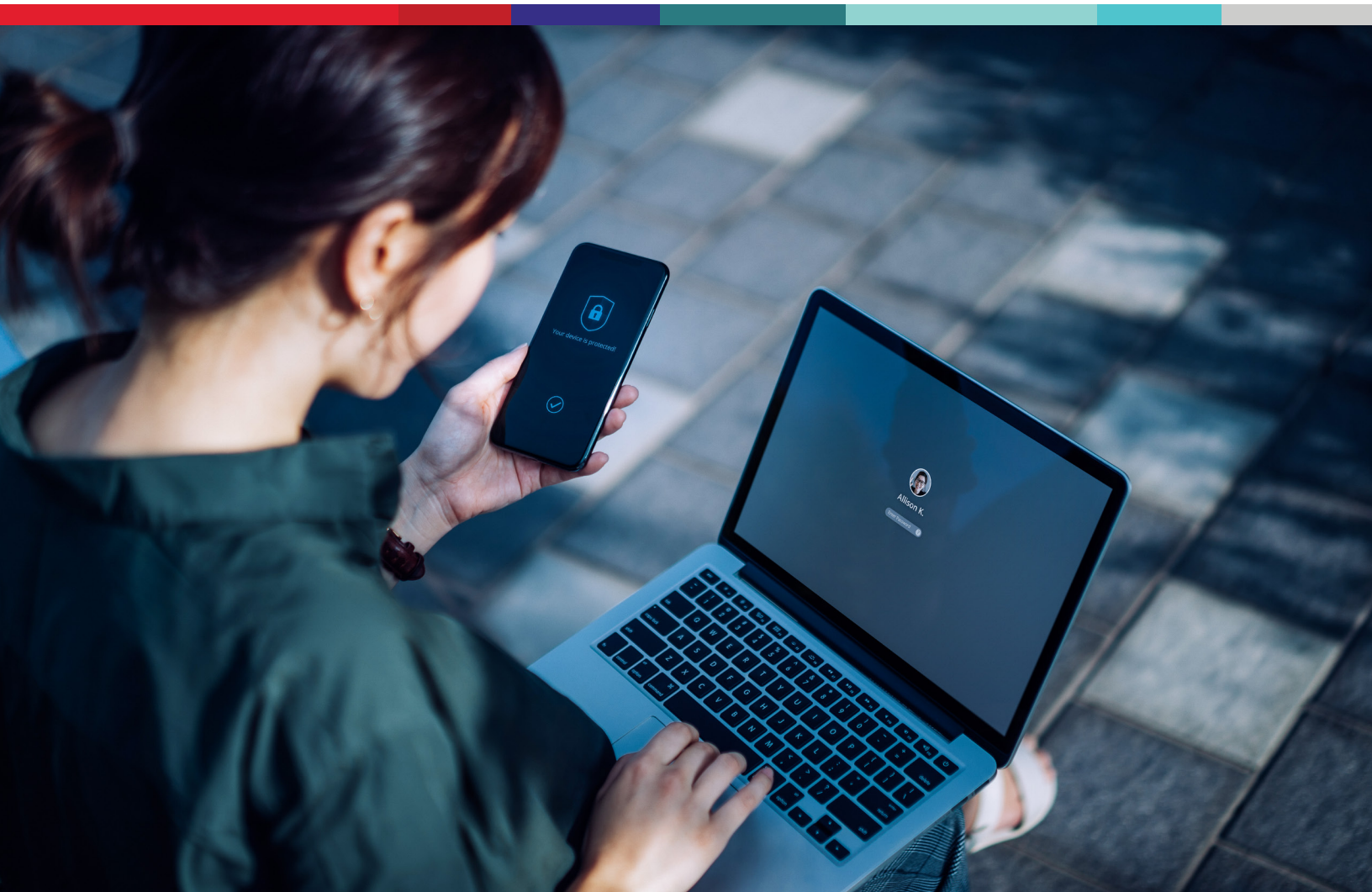
WHITE PAPER

Why Multi-factor Authentication Could be Dangerous for Your Business and Consumers

The deployment of secured authentication elements and deep customer authentication as an outcome of runtime cross functional platforms.



Conditions within which businesses must succeed have never been more challenging. The need to embrace explosive digital transformation is made more complicated by navigating vast solution portfolios offered by vendors. This is further compounded by regulatory and compliance requirements that seek to secure consumers who are moving to and spending more time online than before.

In a business environment where customer behavior is changing, digital transformation is accelerating, the threat of fraud is proliferating and challengers are gaining ground, organizations must change their approach to succeed. A fundamental priority is to find capabilities that offer the opportunity to both reduce bottom-line cost and, by doing so, increase top-line revenue while ensuring compliance. In other words, companies should inspect their portfolios and divest in capabilities that provide only cost-out or revenue-in outcomes in favor of those that do both and at the same time ensure regulations are met. To find these capabilities, C-suite members must be bold enough to ask internal processes owners to think beyond their domains and relentlessly look to solve through cross-functional cost-out and revenue-in capabilities that offer secure ways to transact with their customers.

In an extension to the whitepaper “The New Business Imperative” by Paratha Sarathy and Larry Venter where the authors contended that to be effective in the rapidly transforming digital business world, companies will need to embrace cross-functional capabilities that curb costs and grow revenue, authors Chris Fuller and Larry Venter now shine a light on how runtime cross functional capabilities not only extend business value but also offer unique and exciting ways to creatively solve for regulatory and compliance challenges such as Strong Customer Authentication. They challenge the conventional approach of Multi Factor Authentication as the dominant way to legitimize users suggesting rather that platforms enabling runtime cross functional capabilities offer faster, frictionless and more profitable solutions while considerably improving adherence to regulatory compliance.

SHAPE, AS A CROSS-FUNCTIONAL COST-OUT AND REVENUE-IN PLATFORM EQUIPS CUSTOMERS WITH THE ABILITY TO REDUCE PRESSURE ON THE BOTTOM-LINE AND SIMULTANEOUSLY GROW TOP-LINE REVENUE.

In the following paragraphs, the authors will set out to nullify the reliance on conventional MFA as a secure and compliant mechanism for user authentication required by PSD2. They will surface the concept of Secured Authentication Elements as an outcome of runtime cross functional platforms as alternative or complimentary SCA compliant authentication methods that are more secure and allow you to offer improved customer experience while respecting regulatory necessities. Finally, they will set out the dangers of the prevalent Multi Factor Authentication methods being used today and introduce the reader to the concepts of Simple Customer Authentication and Deep Customer Authentication.

Shape, as a cross-functional cost-out and revenue-in platform equips customers with the ability to reduce pressure on the bottom-line and simultaneously grow top-line revenue. Evolving beyond the synthetic traffic detection and mitigation capability, Shape has developed the ability to reduce human related fraud activity in an unrivaled way, ensuring

that only legitimized users enter your systems and benefit from your investments. Shape's cross functional platform offers a unique opportunity to rethink investments across security, fraud and identity capabilities while providing unparalleled outcomes across said functions.

Payments Services Directive 2 and Strong Customer Authentication

It is expected that by 2023 digital marketing spend will be 60.5% of total media spending at $517.51B worldwide. The main goal of digital ad spend is to drive traffic to their web and mobile channels to provide a personalized consumer experience leading to sales conversion and increased revenue. Organizations are also working to derive maximum benefit from consumer data, leveraging machine learning and artificial intelligence to provide the next best offer and provide a one-click checkout and authentication experiences. In every industry there is a surge in pressure to increase revenue and reduce operating costs and losses. Digital transformation has become imperative. Signaling renewed urgency to increase revenue across the board, IDC estimates organizations will spend $7.4 trillion dollars on digital transformation efforts between 2020 to 2023.

The increased investment and focus on digital transformation have provided a larger attack surface for fraudsters. To combat this, organizations like the European Banking Authority (EBA) have worked diligently to ensure consumer protection through issuances of decrees like the Payments Services Directive 2 (PSD2) which attempts to protect users through Strong Customer Authentication (SCA). Specifically, article 4, Paragraph 30 "strong customer authentication" means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.

Deconstructing Strong Customer Authentication

Before offering a creative, advanced and more secure way of complying with SCA it is perhaps incumbent upon us to look more closely at PSD2 Article 4, Paragraph 30 which outlines the requirements for Strong Customer Authentication.

A cursory consideration of the above would have security and fraud practitioners as well as proponents of frictionless user experiences pondering several questions. Most of these questions introduce a security/fraud vs customer experience conundrum to businesses

and users alike. While security and fraud agents may wonder why for instance most online properties appear to only use two elements to meet regulatory compliance (the literal minimum bar), user experience agents lament the friction introduced by meeting (the literal minimum bar) PSD2 regulatory compliance.

How Does PSD2 Define "Knowledge"

Complaint elements for knowledge are defined as “something only the user knows” and include (but are not limited to):

- Passwords
- PIN's
- Knowledge based response to challenges or questions
- Passphrases
- Memorized swiping paths

Shape security has the ability to gather “knowledge elements” and use them as part of the authentication process in conjunction with other Secured Authentication Elements to validate users should the customer require that as part of their solution.

How Does PSD2 Define "Possession"

Compliant elements for possession are defined as “something only the user possesses” and include (but are not limited to):

- Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS, OTP)
- Possession of a device evidenced by a signature generated by a device (hardware or software token)
- App or browser with possession evidenced by device binding such as (private key linking an app to a device, or registration of the web browser linking a browser to a device)
- Note: approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a device binding process that ensures a unique connection between the PSU's app, browser or key and the device

Shape security has the ability to generate a Device ID that when linked to a Unique User ID creates a link between Device and User. Our Secured Authentication Elements further enhance the bonding between device ID and UUID with other user generated elements and behavioral characteristics that can be used to validate the user.

How Does PSD2 Define "Inherence"

Compliant elements for inherence are defined as “something only the user is”. These elements are related to biological and behavioral biometrics, physical properties of body parts physiological characteristics and behavioral processes created by the body and any combination of these and is the most fast moving and innovative element. Compliance elements for inherence include (but are not limited to):

- Retina and Iris Scanning
- Fingerprint scanning
- Vein recognition
- Face and hand geometry
- Voice recognition
- Keystroke dynamics (identifying the user by the way they type and swipe, sometimes referred to as typing and swiping patterns)
- Heart rate

Shape security uses rich and varied sets of Keystroke Dynamics to inspect behavioral characteristics which when combined with other Secured Authentication Elements such as Device ID can confidently authenticate and score the intent of the user.

The Multi-factor Authentication Myth

What is clear from PSD2 is that the EBA requires Strong Customer Authentication. The EBA also outlines what needs to be done to achieve compliance - authentication based on the use of two or more elements categorized as knowledge, possession and inherence. Nowhere does it suggest that Multi Factor Authentication (MFA) is a requirement. It is likely that MFA and or 2FA has become an umbrella term used by businesses to describe the process of authenticating a user. What is also evident is that compliance through MFA /2FA has becomes synonymous with two of the most prevalent authentication methods used by businesses, namely One Time Passwords (OTP) and Short Message Service (SMS).

There has been debate about the security of SMS as a delivery mechanism for OTP. The EBA rulebook provides some further context:

"In this context, a one-time password sent via SMS would constitute a possession element and should therefore comply with the requirements under Article 7 of the Delegated Regulation, provided that its use is 'subject to measures designed to prevent replication of the elements', as required under Article 7(2) of this Delegated Regulation. The possession element would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number.

PAYMENT SERVICE PROVIDERS SHALL ENSURE THE CONFIDENTIALITY AND INTEGRITY OF THE PERSONALIZED SECURITY CREDENTIALS…

In addition, regardless of whether a strong customer authentication element is possession, knowledge or inherence, Article 22(1) of the Delegated Regulation requires that "payment service providers shall ensure the confidentiality and integrity of the personalized security credentials of the payment service user, including authentication codes, during all phases of the authentication" and Article 22(4) of the Delegated Regulation states that "payment service providers shall ensure that the processing and routing of personalized security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognized industry standards".

The challenge here surrounds the statement that "payment service providers shall ensure the confidentiality and integrity of the personalized security credentials…" Given that SMS messages are delivered in clear text, there are inherent known vulnerabilities in the SS7 protocol used to deliver SMS messages, and examples of mobile malware that are designed to steal text messages from user devices, it seems illogical to require PSPs to ensure integrity while still allowing SMS as an OTP delivery option.

Beyond SMS, we have seen how fraudsters and cybercriminals have changed tactics, targeting the week human link in the authentication chain. Cybercriminals can procure phishing kits and services online (see the recent takedown of the "SMS Bandits" as an example) in order to create convincing mechanisms that persuade end users to divulge their information and rapidly share that data with waiting operatives. Meanwhile, sophisticated phishing kits such as Kr3pto give experienced threat actors the ability to intercept OTPs in real time.

From the above it should be evident that businesses relying on any of the above authentication methods are effectively introducing a security risk and exposing their customers to harmful practices in an attempt to meet SCA regulatory requirements. In contrast, Shape, as the only true runtime cross functional platform, enables Strong Customer Authentication by offering unrivaled authentication services across all three compliant elements required by SCA.

What Does SCA Compliance Typically Look Like Today?

Each reader of this paper has been challenged through either OTP or 2FA as a method of authentication. Where only two elements compliant elements are used to authenticate a user we refer to it as Simple Customer Authentication – meeting the literal lowest bar for compliance.

Below is a schematic of Simple Customer Authentication typically experienced in money transfers for example.

- **Step 1:** User approaches online property or application.
- **Step 2:** Username is either entered or prepopulated (username is not a knowledge element on its own).
- **Step 3:** User enters Password or PIN (a compliant knowledge element).
- **Step 4:** User attempts to transfer money and is stepped-up through the provisioning of a One Time Password or SMS (both compliant possession elements).
- **Step 5:** User enters OTP/SMS and can complete transfer.

In the above authentication flow the bare minimum is done to achieve compliance under PSD2. Two compliant elements are indeed used to authenticate but when considered with an understanding that OTP/SMS is a porous authentication method, businesses deploying this authentication method and users experiencing it should not rest easy. This low-level authentication is an example of Simple Customer Authentication.

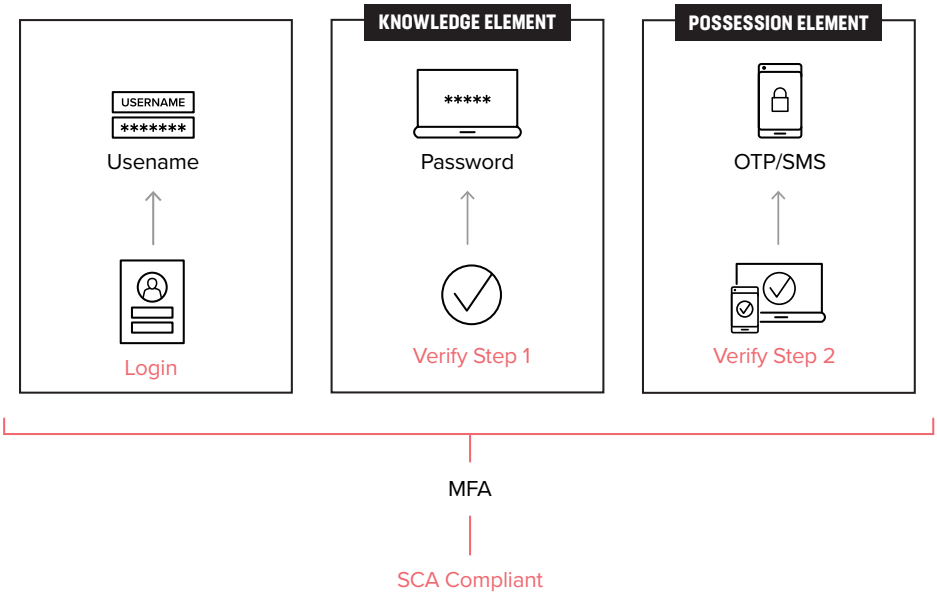


Figure 1: Light Compliance

What Does Deep SCA Compliance Look Like?

By contrast, Deep Customer Authentication as an outcome of runtime cross-functional platforms offers a fresh, more secure and faster method of authentication using three compliant elements. The deployment of Shape's Secured Authentication Elements renders the need for any step-up mechanism unnecessary while remaining compliant with PSD2 and Strong Customer Authentication requirements. With Deep Customer Authentication the customer can choose to authenticate using a "possession element" and an "inherence element" and can even offer a third "knowledge element" to authenticate against.

As acknowledged by the European Banking Authority, the "inherence element" is the most exciting and progressive arena for authentication. In the scenario below two authentication methods are explored as alternatives to the Simple Customer Authentication example for money transfer above:

Method 1–Deep Customer Authentication (3 element verification)

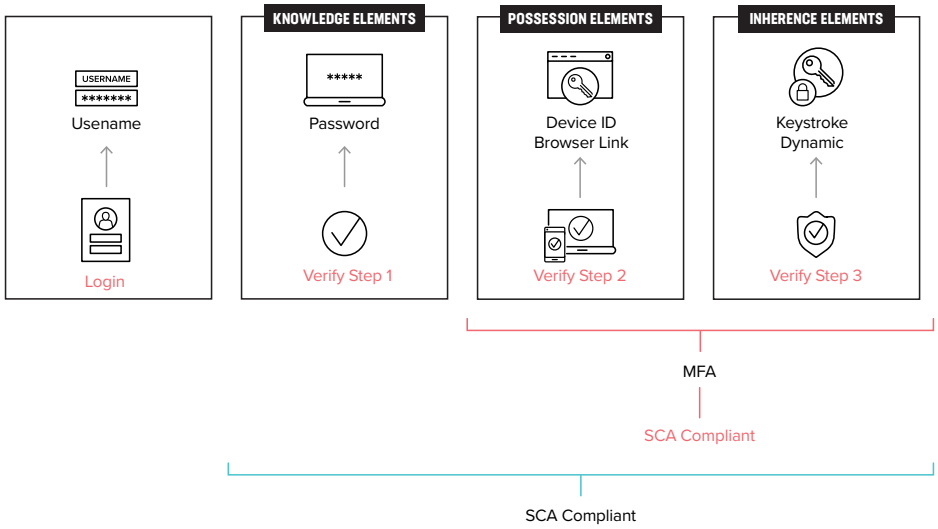
- **Step 1:** User approaches online property or application.
- **Step 2:** Username is either entered or prepopulated (note that username is not a knowledge element on its own)
- **Step 3:** User enters Password or PIN (a compliant knowledge element)
- **Step 4:** Platform performs runtime "possession element" verification through Device ID
- **Step 4:** Platform performs runtime "inherence element" verification through Keystroke Analysis
- **Step 5:** User is verified and completes money transfer with no step-up friction.

Method 2–Deep Customer Authentication (2 element verification)

- **Step 1:** User approaches online property or application.
- **Step 2:** Platform performs runtime "possession element" verification through Device ID
- **Step 3:** Platform performs runtime "inherence element" verification through Keystroke Analysis
- **Step 4:** User is verified and completes money transfer with no step-up friction.

Both flows above are examples of Shape's Secured Authentication Elements being deployed to authenticate a user in compliance with PSD2's Strong Customer Authentication requirements. As and outcome of a runtime cross functional platform Secured Authentication Elements achieve compliance faster, offer a more secure authentication method and remove friction from the user.

Figure 2: Deep SCA Compliance



In Summary

From the above it should be evident that Multi Factor Authentication, as applied broadly today, should be seen as having met the lowest possible bar for Strong Customer Authentication as required by PSD2. Further, as the lowest possible bar of authentication MFA could literally be putting your organization and your customers security in jeopardy. It should also be clear Strong Customer Authentication, not MFA, is the PSD2 regulatory requirement.

Instead, Deep Customer Authentication achieved within the Shape platform offers rigorous cross functional analysis in Security, Fraud and Identity functions. The use of Secured Authentication Elements allows higher fidelity and more flexible authentication methods that align with the SCA compliant requirements of knowledge, possession and inherence.

To learn more, contact your Shape Security or F5 representative, or visit shapesecurity.com or f5.com.