BUSINESS CASE

macro global®
creating value through innovation

Right Authentication Method for Financial Service Provider

Executive Summary

In today's world, fraudulent actions in electronic payments are one of the main threats faced by financial and payment service providers. Open Banking aims to harmonise the payment market players and foster the adoption of innovation and data security to reduce the hurdles in the competitive era. As a core component of opening the payments market to third-party providers (TPPs) through common and secure communication, Open Banking seeks out to strengthen security in payments by mandating SCA. Strong Customer Authentication (SCA) and secure communication are key to achieving the Open Banking objective by enhancing consumer protection mandating new security processes to improve the security of payment services across the UK. Although payment service users (PSUs) have an immense benefit around security and data protection, industry actors (service providers and e-commerce merchants) face new challenges in supporting the legal, functional, technical, and business implications of the Regulatory Technical Standards (RTS).

In this business case, we will discuss the challenges faced by our client in implementing the right authentication method and how Macro Global's SCA service on multi-factor authentication supported the financial service provider to address the inherent risks by minimising the fraudulent threats with the advent of new technology in a secured manner.

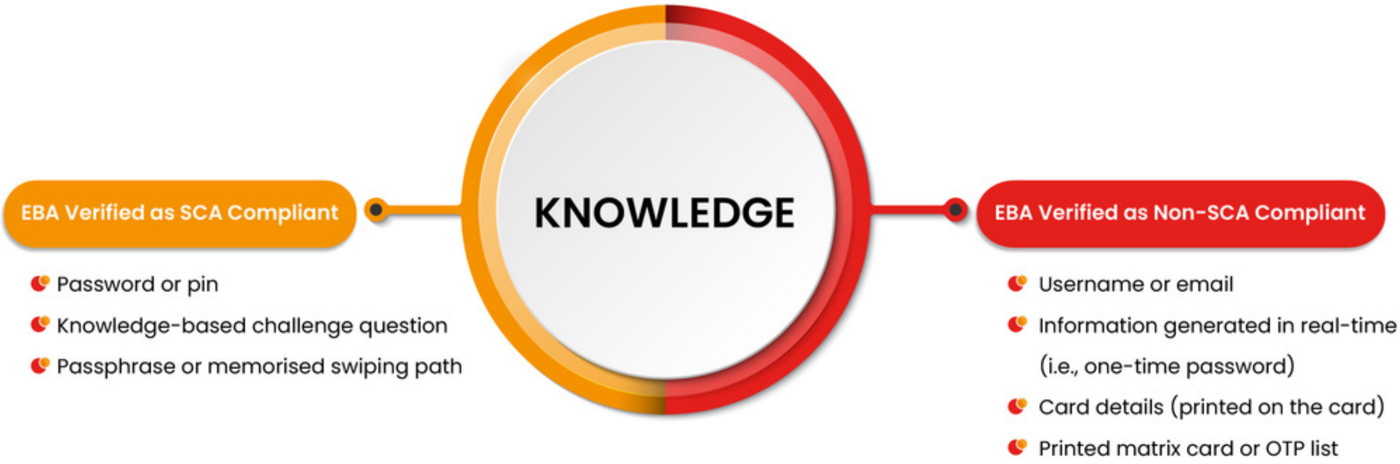
What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a European Regulatory framework defining three types of information that need to be reviewed as part of an electronic payment transaction to improve security. The RTS on Strong Customer Authentication is designed to standardise data security policies and improve the adoption of strong customer authentication processes to ensure the payment journey, protect the data and reduce the risk of fraud.

Strong Customer Authentication (SCA) under Open Banking requires a combination of at least two factors for identification and creates a unique authentication code which dynamically links the transaction. The SCA elements must be independent of each other so that a security breach of one will not compromise another and the SCA authorisation elements consist of:

"Something you know", the KNOWLEDGE Element (e.g., password or PIN)

Acceptable knowledge elements are sets of information that are protected by mitigation measures to prevent disclosure to third parties and that existed prior to the transaction being attempted.



KNOWLEDGE

EBA Verified as SCA Compliant

- Password or pin
- Knowledge-based challenge question
- Passphrase or memorised swiping path

EBA Verified as Non-SCA Compliant

- Username or email
- Information generated in real-time (i.e., one-time password)
- Card details (printed on the card)
- Printed matrix card or OTP list

“Something you have”, the POSSESSION Element (e.g., phone or hardware token)

Possession elements are measured by the generation or receipt of a secure, dynamic validation on a device. Possession elements can be measured by some technologies that do not require active customer interaction (e.g., capturing the unique signature generated by a device) or more commonly by pushing a one-time password to the device via SMS text.

POSSESSION

EBA Verified as SCA Compliant

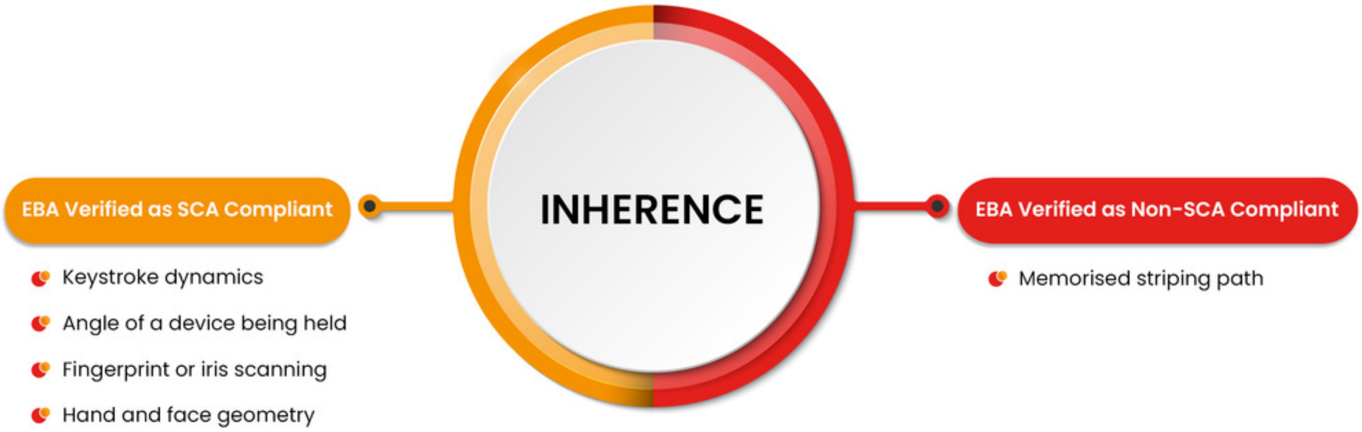
- Signature generated by a device (hardware or software token)
- OTP generated by or received on a device (hardware or software token, or SMS OTP)
- App or browser with possession evidenced by device binding (i.e., through a security chip embedded into a device or private key linking an app to a device)
- Card evidenced by a dynamic card security code
- Card or device evidenced through a QR code (or photo TAN) scanned from an external device
- Card evidence by a card reader

EBA Verified as Non-SCA Compliant

- Installed app without registration
- Card evidenced by card details (printed on the card)
- Card evidenced by a printed element such as OTP list

"Something you are” the INHERENCE Element (e.g., fingerprint or face recognition)

Inherence element consists of measuring data related to the physical properties, physiological characteristics, or behavioural processes of the body.



INHERENCE

EBA Verified as SCA Compliant

- Keystroke dynamics
- Angle of a device being held
- Fingerprint or iris scanning
- Hand and face geometry
- Voice recognition
- Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g., for wearable devices)
- Vein recognition
- Information transmitted using EMV® 3-D Secure

EBA Verified as Non-SCA Compliant

- Memorised striping path

Business Background

Security breaches and cyber-criminals are endless exploring new techniques to exploit vulnerabilities. At the same time, security demands are turned up from Regulators and customers due to the relentless threat of fraud and cyber-attacks hovering around financial service providers to ensure the data are secured.

Under the new directive, service providers must provide compliant authentication processes to meet the payment service user (PSU) needs. Security measures need to be compatible with the level of risk implied in the payment service offering an enhanced user experience. With robust authentication, service providers can deliver the vision of a secure and seamless banking experience and remain compliant with Strong Customer Authentication (SCA) Regulations. Financial service providers should be able to easily integrate the right authentication method for the payment service user by striking the right balance between security and convenience.

Our Clients Problem Statement

Our client (a foreign bank in the UK) is one of the largest financial institutions with strong retail and corporate banking franchise. The bank has emerged as a lead investment financier delivering a range of comprehensive financial services through accessible network, Internet banking and Mobile banking services offering their customer a unique convenience and seamless accessibility for their banking needs.

As a pioneer in the banking industry, our client has been relentlessly improving their services to retain the competitive edge and brand integrity. The bank enables both its retail and corporate customers to manage transactions to their own or third-party accounts via an e-banking solution by providing 24/7 access. Our client wanted to migrate their customers from traditional channels and improve trust in internet banking. The bank desired to create secured accessibility for their customers by implementing a reliable authentication solution and comply with RTS Strong Customer Authentication (SCA) mandates.

The Regulatory Technical Standards (RTS) requires the financial service providers to authenticate the payment service user (PSU) when the user accesses the payment account or initiates payment transaction or performs any action through an internet banking channel that may involve a risk of fraud.

When SCA is Applied?

Accessing the payment account online
Initiating payment transaction
Performing any action through internet banking which may imply risk

Besides the high level of security, internet scam has been increasing over the recent years. The bank had employed the latest technology to deal with the fraudulent threats, given that the bank authentication methods reply on legacy infrastructure and modification to the SCA architecture was complex and expensive. As a financial service provider, our client demanded the right authentication solution to secure their customer's (PSUs) transactions and remain flexible to adapt the strategies around authentication methods as technology evolve. To avoid unauthorised access, the bank was constantly looking out for an intuitive solution by deploying an authentication model to secure data exchange underpinned by real-time identity validation, data analysis and well-informed consent.

Macro Global's Strong Customer Authentication Implementation

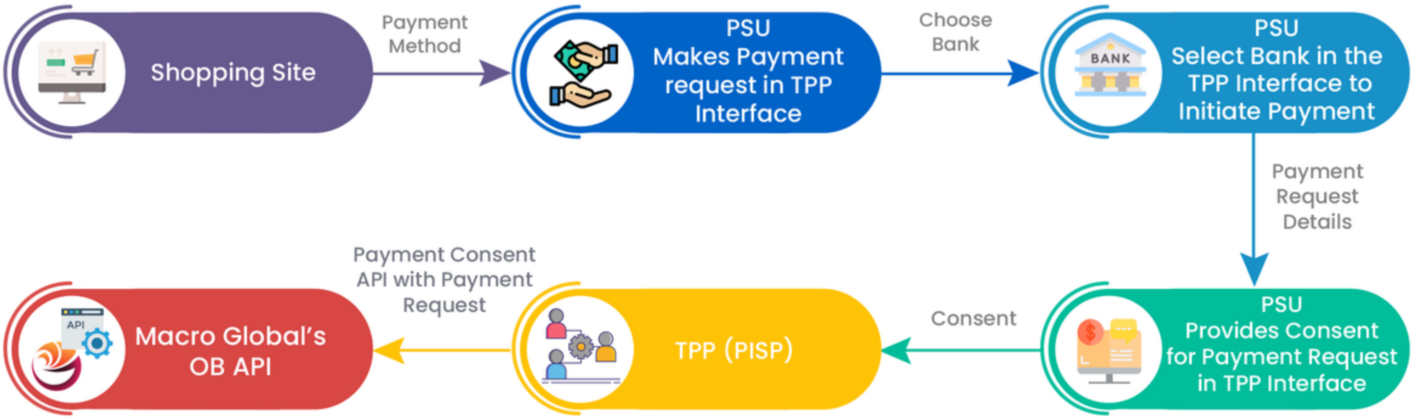
The Regulation landscape is shifting rapidly with the rise of challenges for banks and payment service users (PSUs) expect a fully digital and seamless experience at all touchpoints. A potential solution for Strong Customer Authentication (SCA) would support financial service providers to build an SCA solution as a separate add-on module. Macro Global's Tavas – Open Banking Product Suite and Solutions allows financial service providers to comply with Open Banking requirements and provide secure, strong customer authentication for web and mobile banking applications.

Macro Global's Strong Customer Authentication service is a cloud-based service offering secure, multi-factor authentication and no security-related information is stored on our servers. Payment service user (PSU) authentication is handled securely to prevent data breaches and no credentials are exchanged in the whole form (unlike passwords and two-factor authentication). Macro Global's SCA service creates a streamlined user experience and payment service users can securely authorise the payment.

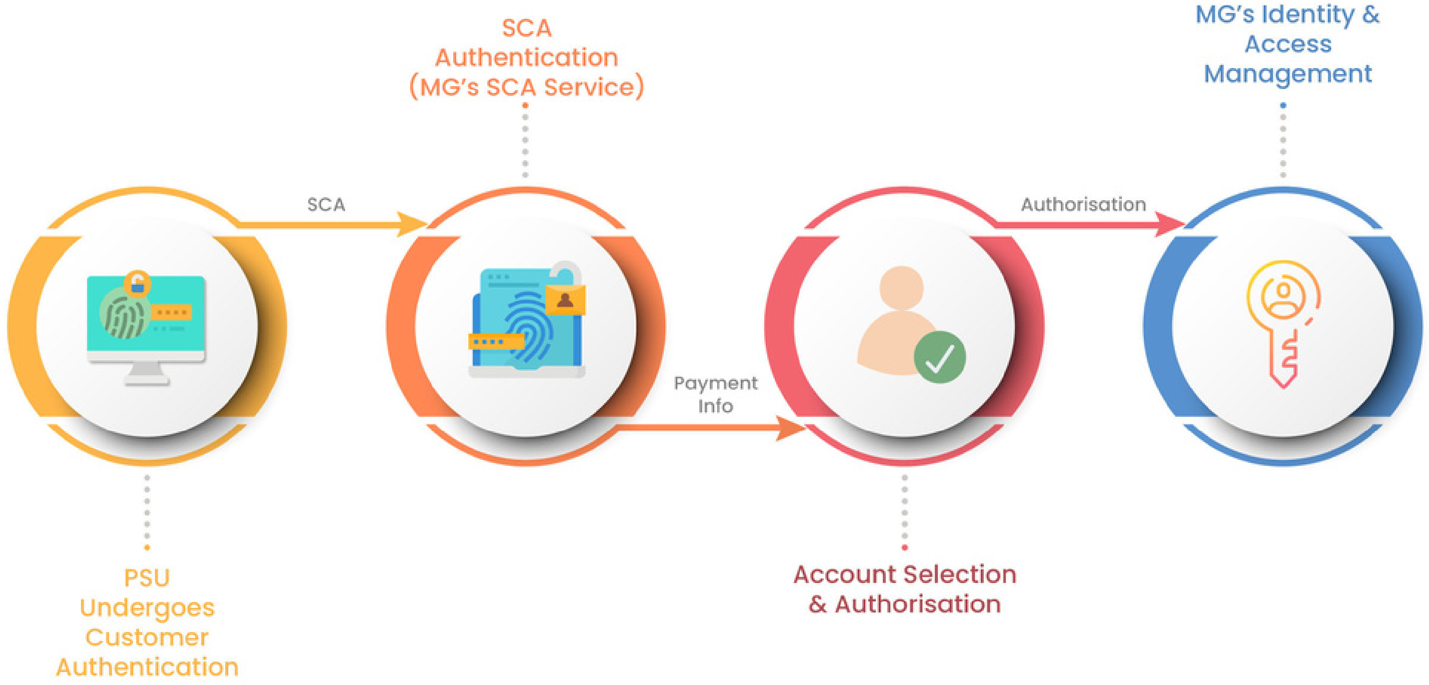
Macro Global's Right Authentication Adoption

Let's head in detail how Macro Global's Strong Customer Authentication service is implemented in a payment flow.

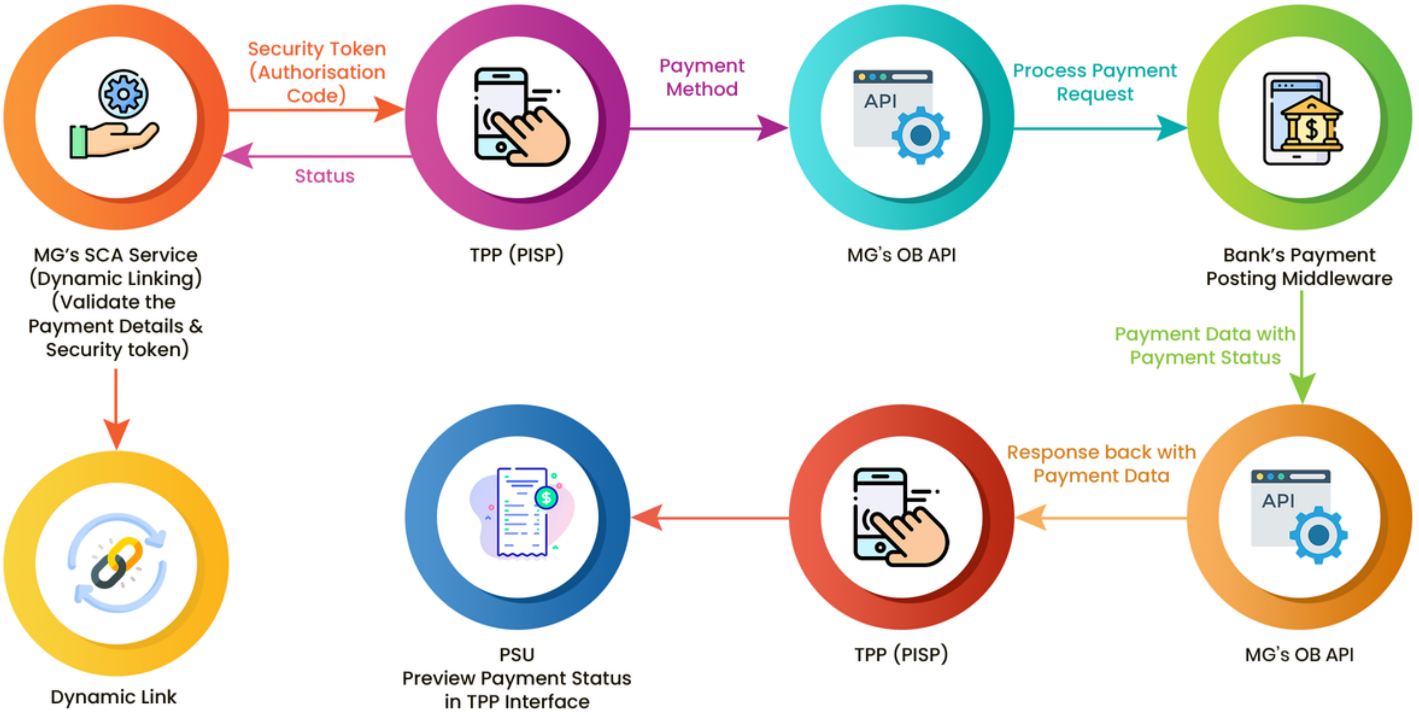
Payment Initiation Consent


Shopping Site
Payment Method
PSU Makes Payment request in TPP Interface
Choose Bank
BANK
PSU Select Bank in the TPP Interface to Initiate Payment
Payment Request Details
PSU Provides Consent for Payment Request in TPP Interface
Consent
TPP (PISP)
Payment Consent API with Payment Request
API
Macro Global's OB API

Authentication Authorisation


SCA Authentication (MG's SCA Service)
MG's Identity & Access Management
SCA
Authorisation
Payment Info
PSU Undergoes Customer Authentication
Account Selection & Authorisation

Payment Execution


Security Token (Authorisation Code)
Status
Payment Method
Process Payment Request
MG's SCA Service (Dynamic Linking) (Validate the Payment Details & Security token)
TPP (PISP)
API
MG's OB API
Bank's Payment Posting Middleware
Payment Data with Payment Status
Response back with Payment Data
Dynamic Link
PSU Preview Payment Status in TPP Interface
TPP (PISP)
API
MG's OB API

1. The payment service user (PSU) purchases assets and initiates payment through the payment initiation service provider (PISP) in the third-party provider (TPP) interface by selecting the bank (ASPSP).

2. TPP requests the payment service user to provide consent in order to accept and process the payment initiation request.

3. PSU provides consent in the TPP interface to initiate payment for the assets purchased.

4. TPP sends the customer consent and payment request to the payment service user's bank (ASPSP).

5. The financial service provider (ASPSP) validates and confirms the payment request.

6. Upon receiving the confirmation, the TPP redirects the PSU to the ASPSPs internet banking website.

7. The payment service user authenticates the payment with their bank using SCA.

7.1 In order to comply with SCA requirements, the PSU must provide the login credentials (username and password).

7.2 The bank (ASPSP) validates the PSUs internet banking login credentials.

7.3 Upon successful validation, the bank notifies the Macro Global's SCA service about the need for an authentication code.

7.4 Macro Global's SCA service generates One Time Password received on the payment service user's device.

8. Upon successful Strong Customer Authentication (SCA) verification by
Macro Global's service, the bank prompts the PSU to select the account from which the payment should be initiated.

9. The bank then sends a confirmation to the payment service user's browser in the form of an authorisation token generated by the
Macro Global's SCA service.

9.1 Dynamic Linking is the process of linking the authentication token to the payment amount and the specific payee of the transaction.

10. Upon successful SCA authentication by Macro Global's service, the third-party provider uses the application programming interface (API) to send a request to the bank to initiate the fund transfer from the payment service user's account.

11. PSU gets confirmation on successful transaction in the third-party provider interface.

Macro Global's Strong Customer Authentication service is an additional security layer that acts as a security element mandated by Open Banking and does not replace the bank's existing authentication solution. The service requires minimal adjustments from the bank side to meet the Strong Customer Authentication (SCA) requirements.

Business Benefits

The path towards SCA compliance has been prolonged with multiple deadline extensions. Strong Customer Authentication (SCA) implementation have crept down to to-do lists during the Covid-19 pandemic. Considering the timelines and effectiveness of SCA implementation, Macro Global has developed the SCA service ensuring security protocols and controls are in place and to future-proof our clients. Macro Global's Strong Customer Authentication service strengthens and speed up the payment transaction in a secured manner and empowers the bank as a strong competitor in the domain of e-commerce payments.

Integration
Cloud-based service offering and easy to implement.

Protection
Protection from payment incidents and reduce fraudulent rates and unauthorised payment scenarios.

Compliance
Multi-factor authentication solution to make the process smoother and meet the Regulatory compliance.

Security
Secured against database breaches and man-in-the-middle attacks.

Experience
Improved end-user experience and increased trust and loyalty with the payment service users.

We are here to help you

If you want to learn more about our products or services or just have a question?

If you need advise from our expert team who understand your business better than our peers?

If you want to know how we transformed businesses using our unparalleled industry and domain expertise?

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

macro global®

creating value through innovation