Modulr

PSD2 Compliance Partner Requirements

A detailed overview of partner compliance with PSD2

v2
March 2023

LONDON
Scale Space, 58 Wood Lane, London, W12 7RZ

EDINBURGH
80 George Street, Edinburgh, EH2 3BU

AMSTERDAM
Weteringschans 165 C, Amsterdam 1017 XD

Modulr

Contents

1. What is PSD2? 3
1.1. Overview 3
1.2. What is a Payment Account? 3
2. Open Banking 4
2.1. Access to payment accounts 5
2.2. Performance & availability of the payment account access interface 5
2.3. Secure communication with TPPs 5
2.4. PSU Consent 5
2.5. PSU Authentication 5
2.6. Treatment of data requests and payment orders 6
2.7. Information on the initiation of a payment transaction 6
2.8. Denying access to providers of AISP/PISP 6
3. Strong Customer Authentication 7
3.1. How is SCA applied? 7
3.2. SCA Common Compliant Pairs 8
3.3. Dynamic Linking 8
Appendix 1 - Further Information 9
Appendix 2 - Payment Account 10
Appendix 3 - Glossary 11

1. What is PSD2?

The Revised Payment Services Directive (PSD2) is the directive issued by the European Commission for improved innovation and increased internet payment safety. The directive is also aimed at making cross border payments in the EU easier and more efficient when payments are made within member states. It also includes the Regulatory Technical Standards (PSD2 RTS). PSD2 was transposed into UK law within the Payment Services Regulations 2017 (PSRs). PSD2 will be used to reference both the applicable payment regulations across the UK and EU.

PSD2 expands on previous legislation in the following areas:

- Increased customer rights in areas including complaints handling, new rules on surcharging and currency conversion
- Enhanced security through Strong Customer Authentication (SCA)
- Allowing third party providers access to account information providing a framework for new payment and account services (Open Banking)

1.1. Overview

Account Servicing Payment Service Providers (ASPSPs) must ensure that there is a PSD2 compliant way to provide regulated Third Party Providers (TPPs) with access to account data and/or payment functionality; where the proposition meets the definition of a “payment account”.

Distributors and Outsourced Partners of Modulr that provide such a payment account to their customers / payment service users (PSUs) are classified as being in-scope of the PSD2 regulations requiring Open Banking access and SCA.

Typically, the app or browser interface that gives access to the PSU to their account is provided by a Partner, rather than Modulr directly. The customer will need to provide consent to access their account information or to authenticate payments. Therefore, these obligations must be fulfilled by the Partner.

Modulr requires all Partners to share exactly how they will achieve and maintain compliance and will not permit Partners to launch whilst their proposition remains non-compliant. Modulr will also oversee the solution for Partners on our ‘Payments Clearing Model’.

1.2. What is a Payment Account?

There are two definitions of a payment account that exist in these different payment regulations:

- PSD2
- Payment Accounts Regulations 2015/Payment Accounts Directive (2014/92/EU)

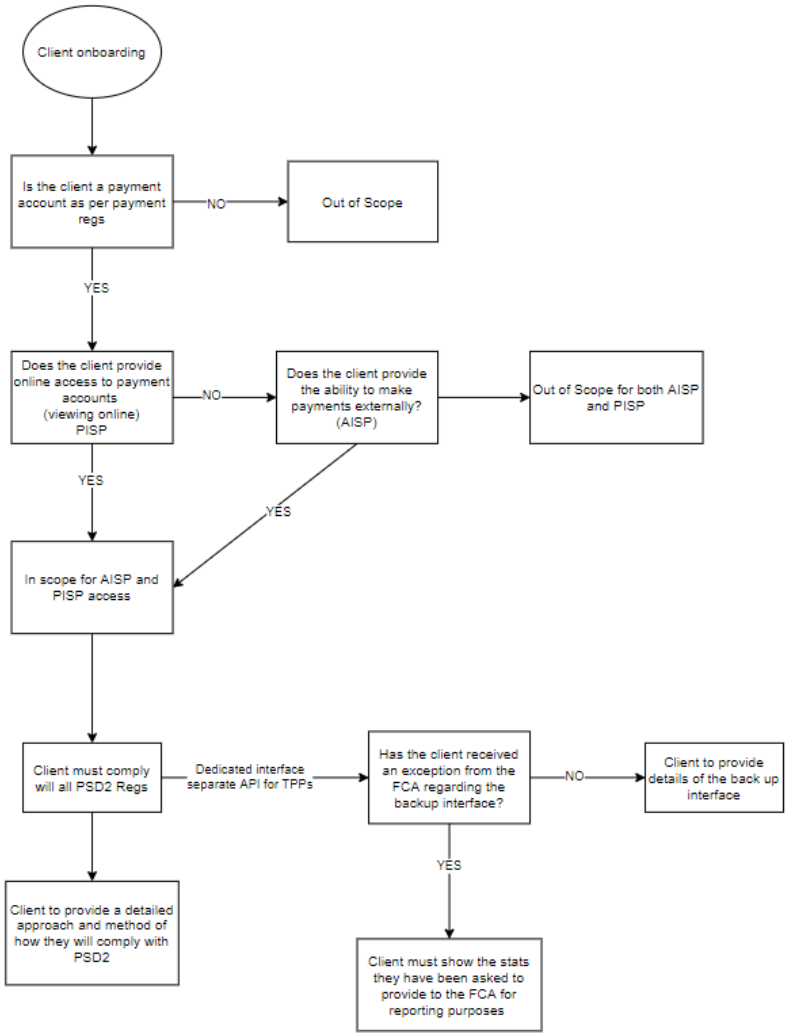
An interface for Open Banking access is required when the customer has access online to a payment account, as per PSD2. This results in a much wider definition when comparing the two and means that more embedded payment solutions are required to implement access to TPPs via Open Banking and SCA.

Modulr will hold discussions and review any submitted evidence whether Open Banking is (or is not) in scope, before signing any contracts. Modulr as the regulated provider, will retain the final decision.

Please refer to Appendix 2 for more information on what constitutes a payment account, as per PSD2.

2. Open Banking

Below is a flow diagram showing the steps needed determine if the client is within scope for Open Banking.



Each Partner must complete the following table:

Are you compliant with the regulatory requirements?		
Answer Option:	**Details for Open Banking**	**Details for SCA**
1. Yes, this company is already compliant.	*Please provide summary of how you are compliant*	*Please provide summary of how you are compliant, including the two factors you have in place*
2. Not yet compliant.	*Please provide your plans on becoming compliant and associated timescales*	*Please provide your plans on becoming compliant and associated timescales*
3. N/A - this company is out of scope of the requirements.	*Please provide details why Open Banking is not applicable to your business or any exemptions you will be relying on*	*Please provide details why SCA is not applicable to your business or any exemptions you will be relaying on*

What are the requirements?

2.1. Access to payment accounts

- Where a 'payment account' is 'accessible online', payment service users (PSU) have a right to use the services of AISPs and PISPs in relation to these accounts
- ASPSPs will only be expected to provide equivalent access to that available directly to their customers (e.g. over the mobile/online channels), no new services are required
- An account which is available online on a 'view only' basis, but without any payment functionality, would only need to be accessible online' for the purposes of AIS (and for delivery of Confirmation of Funds replies to an incoming CBPII request)
- In building the solution, please note that providing access via an API Dedicated Interface is the industry standard.

2.2. Performance & availability of the payment account access interface

- ASPSPs must record and monitor the performance and availability of their payment account access interface. ASPSPs are required to publish performance and availability metrics for their payment account access interface and for direct customer access channels on their website (only applies to dedicated interface).
- ASPSPs must notify the relevant NCA if their payment account access interface becomes unavailable. ASPSPs must activate contingency measures to allow TPPs to continue to access payment account data while the primary payment account access interface is unavailable.
- Modulr will obtain information from Partners to enable its regulatory reporting. Further information can be found here as to the regulatory purpose: https://www.handbook.fca.org.uk/handbook/SUP/16/Annex46BG.html

2.3. Secure communication with TPPs

- An ASPSP must communicate with TPPs in accordance with the security requirements detailed in Chapter V of the RTS on SCA and CSC (CDR 2018/389),
- ASPSP payment account access interface(s) must:
    - Allow TPPs to identify themselves securely through the exchange and validation of TPP eIDAS certificates
    - Enable TPPs to communicate securely to request (and receive) payment account access information or to initiate payments.

2.4. PSU Consent

- PSU consent can be provided directly to the ASPSP or provided via a TPP.
- ASPSPs should not check the terms of the Consent provided by the customer to an authorised TPP, however, these can be displayed to the customer for clarity.

2.5. PSU Authentication

- ASPSPs should allow TPPs to rely on all the authentication procedures that the ASPSP uses to authenticate PSUs when they access their payment account directly.

2.6. Treatment of data requests and payment orders

- An ASPSP must treat data access requests and payment orders that it receives from TPPs the same as those that come directly from its customer unless it has objective reasons to treat them differently.
- For AIS, ASPSPs should make the same information available to a customer via an AISP as would be available to the customer if they accessed their account online directly.
- For PIS, ASPSPs should treat the payment order in terms of timing, priority or charges, as a payment order initiated by the customer directly.

2.7. Information on the initiation of a payment transaction

- Immediately after receipt of a payment order, the ASPSP must provide or make available to the PISP all the same information that is provided to the customer, if the customer initiates a payment through the direct access channel.

2.8. Denying access to providers of AISP/PISP

- An ASPSP may only deny an authorised/registered PISP or AISP access to a payment account for reasonably justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that TPP.
- The ASPSP must notify the relevant NCA of any declines to provide payment account access to authorised TPPs.

Listed below are some technology suppliers in the market that have built PSD2-compliant Open Banking solutions that can work for you. These suppliers are provided as options rather than a formal recommendation because they might be able to help you achieve compliance in shorter timescales.

Please conduct your own due diligence and make your own decisions on an appropriate supplier

- Tell Money
- Saltedge
- Konsentus

Modulr

3. Strong Customer Authentication

SCA is a regulatory requirement to make online payments more secure and aims to reduce fraud. SCA requires all Payment Service Providers (PSPs) to undertake SCA on all in scope actions unless an exemption applies.

SCA must be applied when a payer:

- Accesses their payment account online
- Initiates an electronic payment transaction
- Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses

The above requirements for SCA apply to all electronic payment and card transactions initiated by the payer. SCA also applies regardless of whether the payment service user is a consumer or business.

Typical SCA events are:

- Logging in
- Making Payments out
- Standing Order Setup
- e-commerce transactions (using a card online via 3DSecure)
- Change of Phone Number, Address, Email
- Trusted Beneficiary
- Changing a Card PIN in an online account (as opposed to at an ATM which is not remote)

3.1. How is SCA applied?

SCA is based on the use of two or more independent elements (factors), each of which must be from a different category:

- Something only the customer knows (Knowledge)
- Something only the customer has (Possession)
- Something only the customer is (Inherence)

SCA can also be referred to as 2 Factor Authentication (2FA). However, PSD2 compliant 2FA is only achieved if 2 of three factors are applied independently. You cannot apply the same factor twice (knowledge + knowledge) and be compliant for SCA.

In Appendix 1 there is a link to EBA Guidance Opinion on SCA which covers examples in more detail. It was published in June 2019, so the list is not exhaustive.

Examples of Knowledge Elements:

- Password, mobile PIN (numeric password)
- Knowledge Based Assessment (KBA challenge question), Passphrase
- Memorised Swiping Path

Examples of Possession Elements:

- One Time Passcode (OTP) sent via SMS to a verified phone number
- OTP generated by or received on a device (hardware or software)
- A signature generated by a device (hardware or software token)
- App or browser with device binding or tokens linking to a device

- Card reader

Examples of Inherence Elements:

- Face Recognition, Finger Recognition (Face/Touch ID)
- Heart rate or other body movement patterns (typically wearable devices)
- Voice recognition

3.2. SCA Common Compliant Pairs

- Password and OTP
- Device Binding and Face/Touch ID
- KBA and OTP

How a customer performs login is a key journey because once a consumer is logged in and remains in session, any further in account SCA events that are initiated only require one *further* factor of SCA to be performed. This is due to the regulations allowing one factor from login to be carried over to subsequent journeys (within the same session).

In practice a customer accessing their account with a password and OTP can then make a payment out, with a subsequent OTP dynamically linked to the payment. They don't need to enter the password again. These are two SCA events back to back, but still with two factors each time, Knowledge + Possession and Knowledge + Possession.

3.3. Dynamic Linking

Dynamic linking requires that an authentication code for each transaction must be unique (i.e. it can only be used once), is specific to the transaction amount and recipient, and that both amount and recipient are made clear to the payer when authenticating.

PSD2's dynamic linking requirement specifically states that payment service providers applying SCA:

"shall adopt security measures that meet each of the following requirements:

(a) the payer is made aware of the amount of the payment transaction and of the payee;
(b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;
(c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;
(d) any change to the amount or the payee results in the invalidation of the authentication code generated."

Appendix 1 - Further Information

FCA Approach Document
Payment Services and Electronic Money – Our Approach

SCA is covered under Chapter 20 - Authentication (page 258)

Access to payments accounts is Chapter 17 (page 220)

UK Regulatory Technical Standards
Chapter -3 Application - FCA Handbook

PERG 15
PERG 15 - FCA Handbook

UK Finance SCA Guidance
Strong Customer Authentication | UK Finance

EBA Opinion on SCA
EBA publishes an Opinion on the elements of strong customer authentication under PSD2 | European Banking Authority (europa.eu)

PSD2 Regulatory Technical Standards
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389

Appendix 2 - Payment Account

Questions to determine if the Partner is providing a "Payment Account" to their PSUs

- Does the Partner provide a "Payment Account" that is held in the name of one or more payment services users (PSUs)/customers; which the customer can access online and initiate payments to other third parties?
- Does the Partner provide their PSUs (customers) access to an online account and associated payment functionality or are there restrictions imposed?
- Does the Partner initiate outbound electronic payments from a Modulr account via API which are instructed in their system by a PSU?
- Does the PSU use the payment account to make day-to-day transactions to pay third parties, such as other individuals, their electricity bill, phone bill, etc.

Assessment criteria to determine if a Partner is providing a "Payment Account" to their PSUs

The following factors should be considered when determining whether an account is a "payment account".

- The purpose for which the account is designed and held out;
- The functionality of the account (the greater the scope for carrying out payment transactions on the account, the more likely it is to be a payment account);
- Restrictive features relating to the account (for example, an account that has notice periods for withdrawals, or reduced interest rates if withdrawals are made, may be less likely to be a payment account);
- A limited ability to place and withdraw funds unless there is additional intervention or agreement from the payment service provider (this will tend to point more towards the account not being a payment account); and
- The extent to which customers use an account's payment service functionality in practice.

According to the FCA, in their view:

"payment accounts" can include, for example, current accounts, e-money accounts, flexible savings accounts, credit card accounts, other running-account credit accounts and current account mortgages.

On the other hand, fixed term deposit accounts (where there are restrictions on the ability to make withdrawals), child trust fund deposit accounts and certain cash Individual Savings Accounts (ISAs) are not payment accounts.

We consider only the features of the account used for the purpose of making transactions, to which the regulations apply, fall within scope. For example, in the case of a current account mortgage, the mortgage element of the account would be out of scope, albeit that a mortgage payment from the current account would be subject to the regulations.

In our view, mortgage or loan accounts do not fall within the scope of the regulations. This is on the basis that the simple act of lending funds or receiving funds by way of repayment of that loan does not amount to provision of a payment service.

Modulr

Appendix 3 - Glossary

Account Servicing Payment Service Provider – ASPSP
Is any financial institution that offers a payment account with online access. PSD2 means ASPSP's will have to provide access to let trusted third parties' initiate payments and access account information.

Account Information Service Provider - AISP
Are methods that consumers and companies can use to get a 360-degree view of their finances. PSD2 provides a framework on how these organisations can access customer transaction history and account details.

Card Based Payment Instrument Issuer – CBPII
Is a payment services provider that issues card-based payment instruments that can be used to initiate a payment transaction from a payment account held with another payment service provider.

Payer
A person who holds a payment account and initiates, or consents to the initiation of, a payment order from that payment account; or
Where there is no payment account, a person who gives a payment order;

Payee
A person who is the intended recipient of funds which have been the subject of a payment transaction.

Payment Account
"Payment Account" means an account held in the name of one or more payment service users which is used for the execution of payment transactions. "Payment Transaction" means an act, initiated by the payer or payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and payee.

Payment Initiation Service Provider – PISP
A PISP is any organisation that offers companies, retailers, merchants etc. an online solution for accepting electronic payments. This usually takes the form of software-as-a-service (SaaS) model that connects, for instance, the website of the seller or merchant with the online banking platform of the payer's bank, so a credit transfer can be enacted and completed.

Strong Customer Authentication – SCA
Strong Customer Authentication as defined by EBA Regulatory Technical Standards is an authentication based on the use of two or more elements categorised as knowledge, possession or inherence that are independent and so the breach of one does not compromise the others and is designed in such a way as to protect the confidentiality of the authentication data.

Third Party Provider – TPP
Are organisations that use APIs developed to Standards to access customer's accounts, in order to provide account information services and/or to initiate payments. TPPs are either/both PISPs and/or AISPs.