

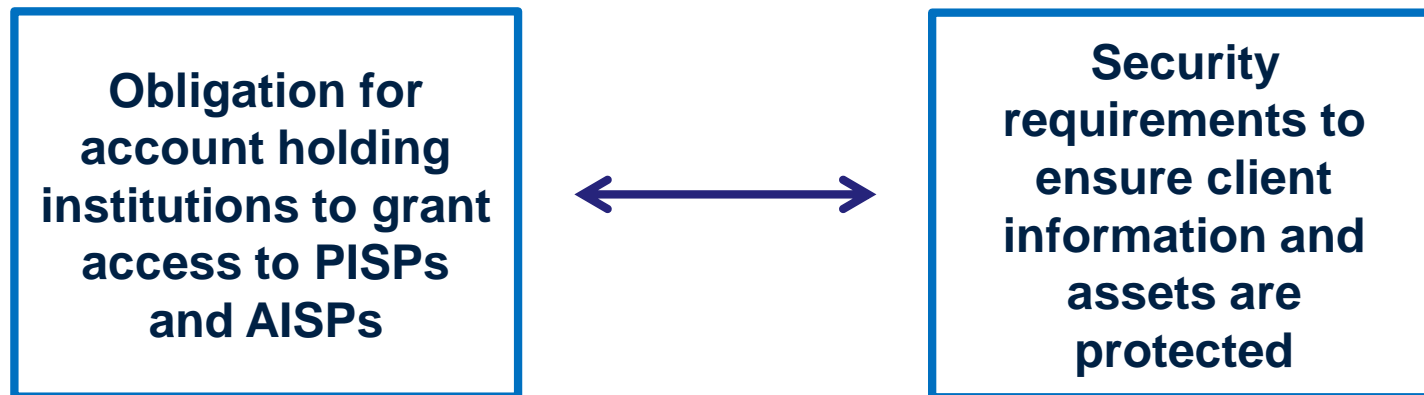


PSD 2

à la croisée de changements juridiques et technologiques

Marc Mouton, Partner, Arendt & Medernach

Access to payment accounts by PISPs and AISPs



Enhanced Security Measures

- Annual assessment of:
 - operational and security risks
 - mitigation measures
 - control mechanisms
- Incident management procedures
 - Notification to regulators
 - Notification to users
- Increased focus during licensing phase



Links with other requirements, i.a.:

- **GDPR**
- **NIS Directive**



R
T
S

- General security requirements: transaction monitoring
- **Strong customer authentication**
- Protection of confidentiality and integrity of users' credentials
- **Common and secure open standards of communication**

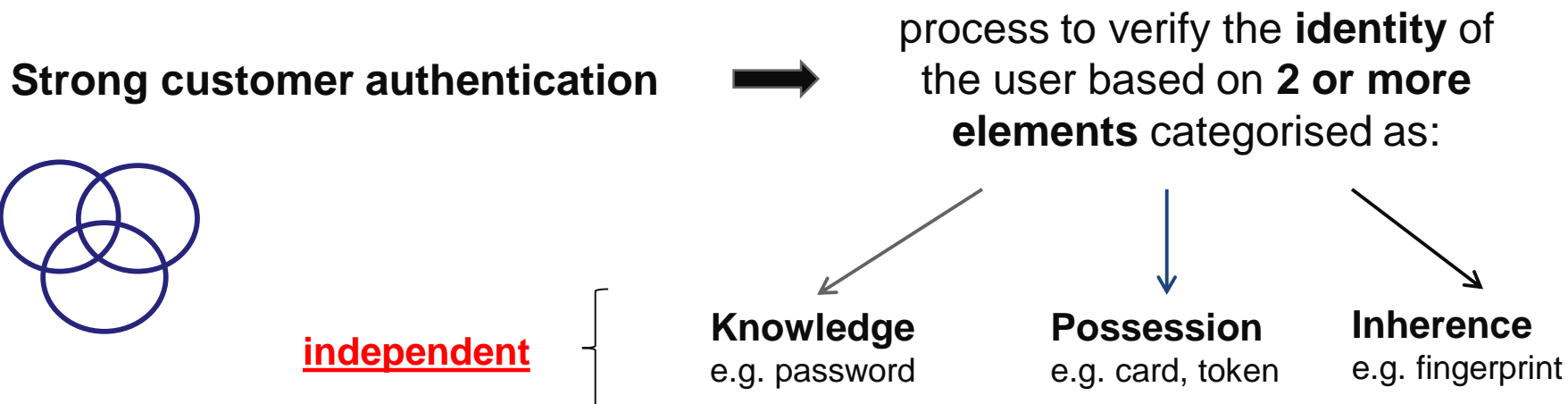


Strong customer authentication




Strong customer authentication

Goal: reduce the risk of fraud + protection of confidentiality



When ? To be performed by payment service provider where the payer:

- accesses its payment account online; or
- initiates an electronic payment transaction; or
-  **dynamic linking of transaction to specific amount and payee**
- carries out an action through a remote channel implying a risk of payment fraud or other abuses.

Strong customer authentication

Exemptions (RTS)

RTS article	Exemption	Payer's PSP	Payee's PSP	
			Credit transfers	Cards
Access to information	Access to payment account information	Yes	N/A	N/A
Article 11	Contactless payments at POS	Yes	No	Yes*
Article 12	Unattended terminal for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payment processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether or not to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction if technically feasible or decline the initiation of the transaction.

Source: EBA Opinion of 13 June 2018



Monitoring obligation!

Strong customer authentication

Category	Description	Examples provided by EBA
Knowledge	Something only the user knows	<ul style="list-style-type: none"> • <u>Compliant</u>: a password, a pin, knowledge-based challenge questions, passphrase, memorised swiping path • <u>Non-compliant</u>: email address or user name, card details printed on the card or OTP generated by, or received on, a device
Possession	Something only the user possesses This category includes both physical and non physical possession	<ul style="list-style-type: none"> • <u>Compliant</u>: a mobile phone, hardware or software token, mobile apps, web browsers or the exchange of keys provided that they include a device-binding process that ensure a unique connection, card evidenced by a card reader or by a dynamic card security code (device requires generation/receipt of dynamic validation element) • <u>Non-compliant</u>: card with possession evidence by card details printed on the card
Inherence	Something the user is This category includes biological and behavioural biometrics, related to the physical properties of body parts; physiological characteristics and behavioural processes created by the body and any combination of these	<ul style="list-style-type: none"> • <u>Compliant</u>: retina and iris scanning, vein recognition, face and hand geometry, voice recognition, fingerprint scanning, keystroke dynamics, angle of holding device, heart rate. • <u>Non-compliant</u>: memorised swiping path (could possibly be a knowledge element), information transmitted using a communication protocol such as EMV 3-D Secure (not an inherence element at this stage because it does not include biological and behavioural biometrics but that could change in the future)

NB.: Compliance dependent on implementation approach

Strong customer authentication

Timing: deadline for implementation in principle 14 September 2019

Exception: extension for e-commerce card payment transactions

Conditions: inform CSSF and submit migration plan to CSSF which includes i.a. the communication initiatives to inform and involve merchants/users

Timetable: to be announced after coordination at EU-wide level

Strong customer authentication

Selected EBA Guidance

- SCA applies to all payment transactions initiated by a payer, including to **card payment transactions** that are initiated through the payee within the EEA (& only on a best-efforts basis for cross border transactions with one leg out of the EEA – essentially to part within EEA).
- An element used for SCA can be **reused** within the same session when initiating a payment, if other element is carried out at payment initiation and dynamic linking condition is met regarding such other element.
- **Direct debit** transactions are not subject to SCA as they are initiated by the payee. However, setting up the mandate via a remote channel (e.g. e-mandate) is subject to SCA if a PSP is involved.
- Where the payer has given a **mandate** authorising the payee to initiate transaction through a payment instrument (**card**), where the mandate is based on an agreement between the payer and that payee for the provision of products or services, the transactions initiated thereafter by the payee are not subject to SCA if no action by the payer is required. However, setting up the mandate via a remote channel is subject to SCA.

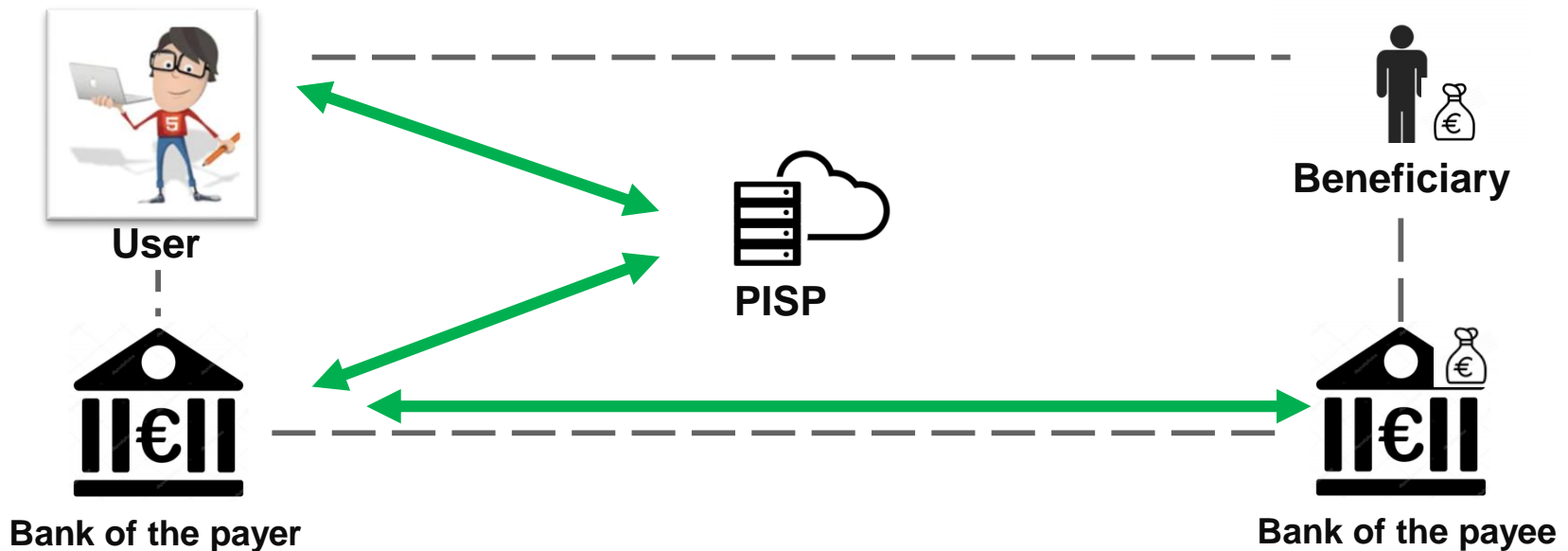


Common and secure open standards of communication

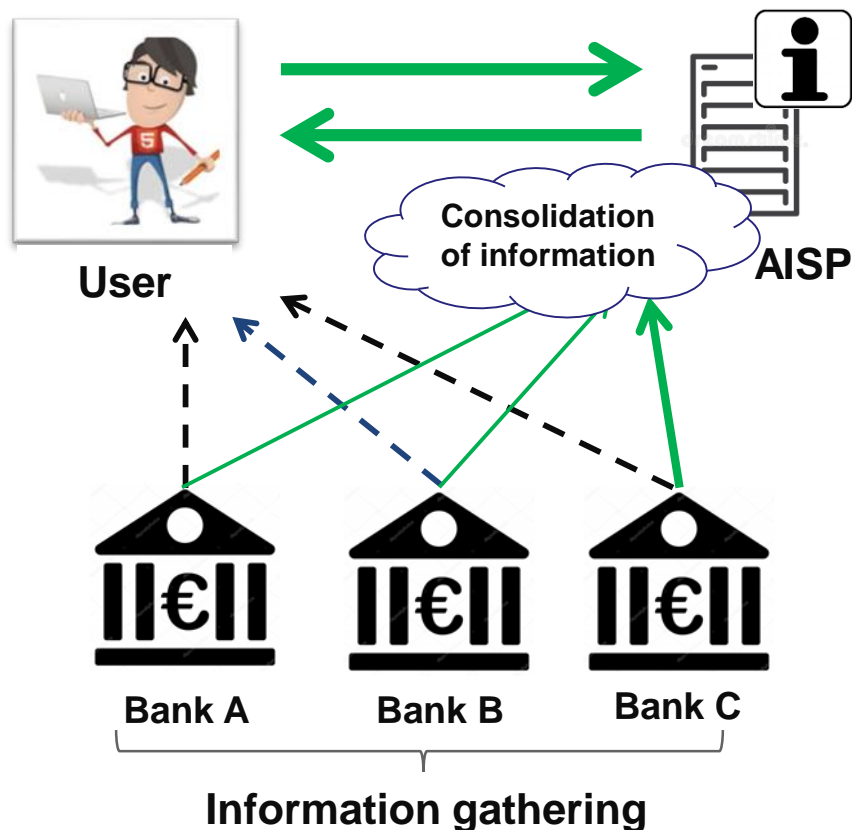


Payment Initiation Service Providers (PISPs)

- Service allowing the initiation of payments from a payment account the user holds with a different payment service provider
- Idea: allow consumers shopping online to pay through a simple credit transfer from their payment account instead of using cards



Account Information Service Providers (AISPs)



- Service consisting in providing users with consolidated information about payment accounts they hold with other payment service providers
- Idea: allow consumers and companies to have a consolidated view of their financial situation

Scope

- Applies to the provider, where the **payment accounts** of the user are **accessible online**
 - regardless of whether the access offers consultative or transactional services
 - irrespective of:
 - a potential disinterest of users to use PIS or AIS
 - the size of the provider and the number of its clients
 - the fact that the provider only has corporate clients
 - the fact that the payment account only allows transactions to an account of the user held with another provider

Opening up access to accounts to TPPs (i)

- PSD2 enshrined the right of TPPs to access payment accounts held with account servicing payment service providers (**ASPSPs**), based on the payment service user's (**PSU's**) explicit consent
- Each ASPSP must offer at least one access interface for TPPs:
 - a **dedicated interface (API)**, or
 - can be only one dedicated interface for all customers or separate dedicated interfaces for different customer segments
 - an **adapted user interface**
 - i.e. the interface also used by clients but adapted so as to allow the TPP to identify itself
- Key obligations (applying to both types of interfaces) include:
 - making technical documentation available at least 6 months before go-live
 - offering a testing facility at least 6 months before go-live
 - requiring qualified eIDAS certificates for identification of TPPs

Opening up access to accounts to TPPs (ii)

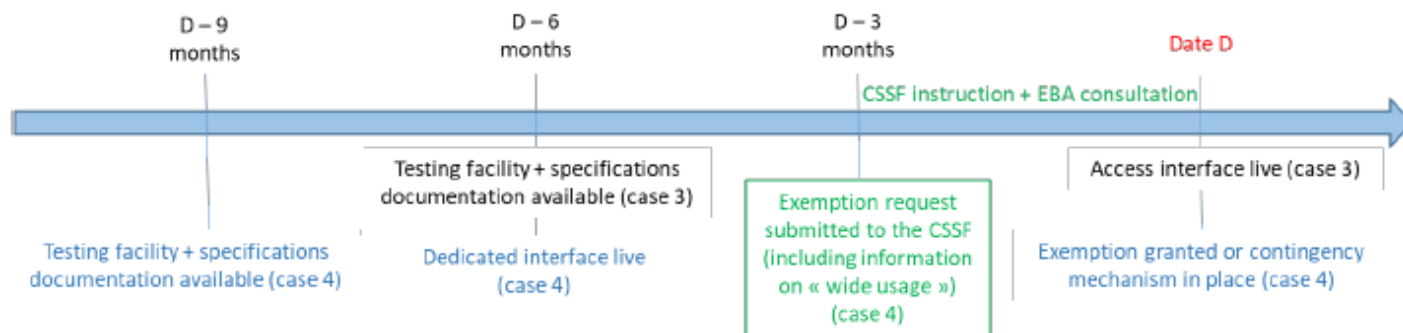
- In addition, those offering a **dedicated interface** must also implement a **contingency mechanism** (fall back mechanism)
- An exemption can be requested from the CSSF in writing
 - specific form to be used
 - specific conditions apply (EBA guidelines available)
 - key condition: three month wide usage testing phase during which dedicated interface has been rolled out into production
- In case third party solution for dedicated interface is used: amounts to material outsourcing

Opening up access to accounts to TPPs (iii)

- Timeline with regard to new offerings of payment accounts available online according to CSSF

The ASPSP plans to offer payment accounts that are accessible online after 14 September 2019 as from day D and:

- either the ASPSP does not want to obtain an exemption from the obligation to set up a contingency mechanism (case 3 – see RTS deadlines);
- or the ASPSP wants to obtain an exemption from the obligation to set up a contingency mechanism (case 4 – see deadlines considering RTS deadlines + time needed for CSSF instruction and EBA consultation).



Source: CSSF Communiqué 28/02/2019

N.B. for changes to existing interface, documentation must be available three months prior to implementation, except in emergency situations

Main sources

- Directive (EU) 2015/2366 on payment services in the internal market (**PSD 2**)
- Law of 10 November 2009 on payment services, as amended
- Commission Delegated Regulation (EU) 2018/389 supplementing PSD 2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (**RTS on SCA and CSC**)
- EBA Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) of 23 February 2017
- EBA Opinion on the implementation of the RTS on SCA and CSC of 13 June 2018
- EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) of 4 December 2018
- EBA Opinion on the use of eIDAS certificates under the RTS on SCA and CSC of 10 December 2018
- EBA Opinion on the elements of strong customer authentication under PSD 2 of 21 June 2019
- CSSF Communiqué of 28 February 2019 on Obligations regarding Strong Customer Authentication and Common and Secure Standards of Communication under Commission Delegated Regulation (EU) 2018/389
- CSSF Circular Letter 19/720
- CSSF Communiqué of 30 August 2019 on the Extension beyond 14 September 2019 of the deadline for compliance with the strong customer authentication (SCA) requirements of Commission Regulation (EU) NO 2018/389 for e-commerce card payment transactions
- Single Rulebook Q&A



Case law



Case law (i)

■ ECJ, 5^o ch., 4 Oct. 2018, case C-191/17, ING-DiBA AG

□ Interpretation of payment account under PSD (same definition under PSD2)

- **Context:** a Bank offers online savings accounts from which its customers can make payments and withdrawals by way of telebanking. These transfers must always be made through reference accounts opened on behalf of those clients. Those reference accounts are current accounts which those clients may also hold with a bank other than the Bank offering the savings account. The online savings accounts require no notice, which means that customers may use the sums paid into those accounts at any time without negative repercussions on the interest generated.
- **Question submitted to ECJ:** whether a savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by way of a current account, called a 'reference account', comes within the concept of 'payment account'.
- **ECJ:** "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.
- "The mere name of an account as a 'savings account' is not sufficient in itself to exclude the categorisation of 'payment account' and the determining criterion for the purposes of that categorisation lies in the ability to perform daily payment transactions from such an account".
- "An account from which such payment transactions cannot be made directly, but for which use of an intermediary account is necessary, cannot therefore be regarded as being a 'payment account' within the meaning of the Payment Accounts Directive and, consequently, within the meaning of the Payment Services Directive."
- "A savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account does not come within the concept of 'payment account'"

Case law (ii)

- ECJ, 3^o ch., 25 Jan. 2017, case C-375/15, BAWAG
 - Information transmission to clients via electronic mailbox of an online banking website
 - **Question:** is information transmitted by the payment service provider to the user of those services through the electronic mailbox of an online banking website, to be considered to have been provided on a durable medium, or merely to have been made available to that user.
 - **ECJ:** “two methods of transmitting information to the payment service user should be distinguished: either the information concerned should be provided, i.e. actively communicated by the payment service provider without further prompting by the payment service user, or the information should be made available to the payment service user, taking into account any request he may have for further information. In the latter case, the payment service user should take some active steps to obtain the information, such as requesting it explicitly from the payment service provider, logging into a bank account online or inserting a bank card into a printer for account statements”
 - “the information concerned which is transmitted by the payment service provider to the user of those services by means of an online banking website may be considered to have been provided [...], if such a transmission is accompanied by active behaviour of the provider aimed at drawing the user’s attention to the existence and availability of that information on that site.”
 - NB: contains also details on conditions to be met for a website to qualify as durable medium.

Contact us



Marc Mouton

Partner

Banking and Financial Services

Tél: +352 40 78 78 336

Email: marc.mouton@arendt.com