Payment Authentication (SCA) using EUDI Wallets - Implementation Guide

USING THE EUROPEAN UNION DIGITAL IDENTITY WALLET (EUDIW) FOR STRONG CUSTOMER AUTHENTICATION (SCA) DURING CARD OR ACCOUNT ONLINE PAYMENTS

Document properties

Name	Payment Authentication (SCA) using EUDI Wallets
Document Version	1.01
Status	Approved
Publication date	October 17, 2024
Contact	EURotterdamTrainingAndDoc@visa.com
Authors	Marie Austenaa, Laurent Bailly, Stan van Haasteren, Stefan Kauhaus, Adam Mansfield, Ranjiva Prasad, Jan Van Vonno

Legal notices

The information, materials and any recommendations contained or referenced in this document (collectively, “Information”) is furnished to you by the EU Digital Identity Wallet Consortium ("EWC", https://eudiwalletconsortium.org/) Payment Taskforce for informational purposes only.

While we aim to provide accurate and up-to-date information, the EWC and/or EWC Payment Taskforce is not responsible for errors in or omissions from this document. The Information is provided “AS-IS” and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. The EWC and/or EWC Payment Taskforce make no warranty or representation of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the Information, products, services, or related graphics contained in the document for any purpose, nor assumes any liability or responsibility that may result from reliance on or use of such Information.

Benefits/results are illustrative only and depend on business factors and implementation details. Any reliance you place on such Information is therefore strictly at your own risk. In no event will the EWC and/or EWC Payment Taskforce be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising, including from loss of data or profits arising out of, or in connection with, the use of this document or the Information.

The trademarks, logos, trade names and service marks, whether registered or unregistered, are the property of their respective owners, are used for illustrative purposes only and do not necessarily imply product endorsement or affiliation unless the Information indicates otherwise.

Please note that the Information may be updated or changed without notice, reflecting our ongoing efforts to provide the most current and useful information. By using the Information in this document, you agree to these terms.

Version History

Version	Date	Changes	Status
0.1	21st of February 2024	Created first draft based on Epics produced in 2023	Draft
0.2	28th of February	Added a lot of content	Draft
0.3	1st of March	Accepted edits and reformatted and reworded as agreed	Draft
0.4	7th of March	Changed the formatting of diagrams	Draft
0.5	19th of March	Made various edits based on reviews	Draft
0.6	2nd of April	Updated registration flows and UX diagrams	Draft
0.7	5th of April	Added section on redirection methodology	Draft
0.7.1	15th of April	Replaced UX diagrams (colour coding) and replaced flow diagram Visio with JPEG	Draft
0.7.2	17th of April	Corrected flow in 3.3.2. Added note about detailed flow diagrams being in 'draft' mode	Draft
0.7.3.	4th of June	- Feedback actioned where applicable - Updated high level flows and pre-reqs to reflect the specification work on RFC007 - Updated the UX to reflect high level flows - Removal of the detailed flow diagrams in the Appendix and instead left place holders for references to RFCs	Draft
0.8	7th of June	- Last changes based on reviews	Draft
0.9	21st of June	- Amendment to registration flow B to align with RFC007	Draft
0.95	12th of July	- Changed template, updated chapter 1, added EWC Payment taskforce description - Editorial updates and improvements - Added UX example to 3.3.2 - Incorporated feedback from Payment Taskforce	Draft
1.0	19th of July	- Incorporated feedback from Payment Taskforce on Dynamic Linking - Fixed formatting issues	Approved
1.01	21st of October	- Updated look and feel of diagrams - added CC licence and authors - updated Payment taskforce (appendix) - updated document title	Approved

Co-funded by the European Union

Co-funded by the European Union

1.Overview

1.1 Background

EWC Consortium[1] has been selected by the European Commission to experiment through Large Scale Pilots the EUDI Wallet in Travel, Business and Payment scenarios.

EWC has formed in 2023 its Payment Taskforce, led by Visa, with the objective of

- defining the EUDI Wallet payment specifications, build and pilot selected payment use cases
- identify barriers to adoption and evaluate opportunities in payment beyond Strong Customer Authentication, in particular by provisioning a card or account token in the EUDI Wallet and initiate an online or in-store payment
- use those specifications and findings to give feedback and offer inputs to the European Commission and future Payment and/or Digital Identity standards

This document is one of the deliverables of EWC's Payment Taskforce - More details and a list of EWC's Payment Taskforce members can be found in Appendix A.1.

1.2 Scope

This document describes the functional specifications of the EUDI Wallet for registration (section 2) and implementation of SCA (Strong Customer Authentication) using the EUDI Wallet in both card (section 3) and account (section 4) online payment use cases.

- this document only covers using the EUDI Wallet for SCA, not the financial transaction itself. Once the SCA is completed using the EUDI Wallet, the actual money movement needs to be performed: authorization and clearing/settlement for card payments, credit transfer SCT/SCT Inst for account payments
- this Implementation Guide aims to give a high-level overview. More detailed flows and technical specifications are described in the Request for Comments (RFC) developed by EWC Payment Taskforce
- It is also possible to provision card or account tokens in the EUDI Wallet. The EUDI Wallet is payment-enabled, and the stored tokens can be used to initiate a payment. This scenario is described in a separate Implementation Guide

1.3 Regulation context

As defined in the Article 5f.2 of the new eIDAS2 regulation that entered into force on the 20th May 2024[2], private relying parties such as banks shall also accept the use of European Digital Identity Wallets for strong user authentication. The Regulation also states an intention (Recital 62) that the regulatory requirements will support strong customer authentication requirements for online identification for the purposes of initiation of transactions in the field of payment services.

Regardless of the ongoing formal legislative approval process, or additional regulatory clarity on these provisions being given, we will assume in this document that banks will have to propose the EUDI Wallet to their customers as an alternative method to perform SCA for online banking login and online card or account payments by the 21st November

[1] **EWC** (European union digital identity Wallet Consortium): Consortium co-funded by the European Union to participate in the large-scale pilots to ensure interoperability and adoption of the European Digital Identity Wallet (learn more at https://eudiwalletconsortium.org/)

[2] https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Co-funded by the European Union

2027 (36 months after the publication of the first Implementing Acts expected on the 21st November 2024), and that the EUDI Wallet must be able to perform strong customer authentication (SCA) for online payments in compliance with:

- the European Union (EU) Payment Service Directive 2 (PSD2) and Regulatory Technical Standards on Strong Customer Authentication and Secure Communications (RTS on SCA) and, as it becomes in effect,
- the EU PSD3, the Payment Service Regulation (PSR) and the to be updated RTS on SCA.

According to the above regulations, the application of SCA is required on every online payment transaction unless the transaction is out of scope or exempted. It requires that the payer is authenticated through at least two factors, each of which must be independent from the other, from two of the three categories listed below:

- Something the payers know (knowledge factor, e.g. a PIN code)
- Something the payer has (possession factor, e.g. a mobile phone)
- Something the payer is (inherence factor, e.g. biometric)

SCA takes place at the end of the shopping experience when the final amount of the basket is known and is ready to be paid. It must be a smooth user experience for both the payee (e.g merchant) and the payer, balancing security with convenience while being compliant with the Architecture and Reference Framework (ARF) and the payment regulations quoted above.

The payer's Payment Service Provider (PSP) is responsible for SCA compliance, ensuring that the two-factor authentication is correctly performed. If SCA cannot be completed (too long, too complex, fails) the payment transaction is declined by the payer's PSP, resulting in the payer not purchasing their desired goods/services and the merchant not converting the sale.

1.4 Audience

This document is aimed at:

- European Commission ARF (Architecture and Reference Framework) experts drafting detailed specifications to enable EUDI Wallet for SCA,
- EUDI Wallet providers who need to know how to enable SCA on their EUDI Wallet,
- Payer's PSP (e.g. Banks) and their authentication services providers (such as ACSs) who must ensure they can use EUDI Wallet for SCA on their card and account payment transactions, and
- Payee (e.g. Merchant) and payee's PSP (e.g. Acquirer) who are looking for implementing new SCA capabilities based on EUDI Wallet on their card and account payment transactions.

1.5 Terms and Actors

Access Control Server (ACS): A provider, to a card issuer/PSP, of authentication services using the EMV 3DS protocol. It receives authentication requests from the 3DS Directory Server (DS), to process those requests on behalf of the card issuer.

Account Servicing Payment Service Provider (ASPSP): Defined in PSD2 to designate the payment service provider (PSP) that holds the payer's account used to fund the payment. This can be a credit institution that provides payment services (i.e., "bank"), an electronic money institution, or a payment institution harmonised to hold customer funds.

The ASPSP is the entity that enforces SCA and executes the payment initiated by the Payment Initiation Service Provider (PISP). For the SCA, it is assumed that the EUDI Wallet is automatically activated using an app-to-app redirection (when on the same device); or using a QR-code when on different devices (e.g., desktop-to-mobile handover); or where multiple EUDI Wallet are registered, to allow user to select the preferred option from a list; or activates the EUDI Wallet once receiving the payment order from the PISP.

Throughout this document the ASPSP is referred to with the more generic term PSP.

Architecture and Reference Framework (ARF): Provides all the specifications needed to develop an interoperable EUDI Wallet Solution based on common standards and practices.

EWC | Co-funded by the European Union

Attestation: A signed set of attributes, see Electronic Attestation of Attributes (EAAs)

Payment Wallet attestation: Attestation issued to an EUDI Wallet instance by a QEAA provider and which confirms that the instance can be used for SCA by the user of the instance.

Card credentials: A user's card details (also called card credentials) can take two different formats:

- **Primary Account Number (PAN):** The "long" number (usually 16 – digits) written on a payment card or
- **Payment Token:** A unique identifier generated by a card network as a proxy for the PAN, which can be used (as an option) by a merchant or their payment service providers to store the card number in their system for future use. This provides enhanced security. Note that a payment card can be physical (e.g. a traditional piece of plastic) or virtual (a digital number only).

Card-Based Payment Instrument Issuers (card issuer for short in this document) – European entity who issues a payment card to a user and who is responsible to ensure SCA is completed. A Card issuer is often an entity commonly referred to as a "Bank" but can also be another type of entity.
Card Network: A payment network that links cardholders, merchants, and card issuers to facilitate electronic payments. Examples of card networks include Visa, MasterCard, American Express, Bank Axept, Cartes Bancaires. The network provides rules and maintains systems enabling the functions performed by various stakeholders in the authentication (identity) and authorisation (blocking of funds) process.

Card Network Directory Server (DS): When EMV 3DS technology is used in the authentication process, it receives authentication requests from merchants and forwards them to a card issuer's ACS for processing/decision. It then communicates the result back to the merchant.

Electronic Attestation of Attributes (EAAs): An attestation in electronic form that allows the authentication of attributes – eIDAS Regulation amendment proposal.

European Union Digital Identity Wallet (EUDI Wallet**) or basic** EUDI Wallet**:** The EUDI Wallet instance used to authenticate the user for a specific transaction (amount and payee/merchant name) and sends the result back to the user and to the authentication requestor. The requestor may be an ACS or a merchant depending on which of the technical flow is used.

European Union Digital Identity Wallet (EUDI Wallet) **instance**: Instance of an EUDI Wallet bound to the User's device.

European Union Digital Identity Wallet (EUDI Wallet**) provider:** Provider (or issuer) of EUDI Wallet instances to users.

EWC (European union digital identity Wallet Consortium): Consortium co-funded by the European Union to participate in the large-scale pilots to ensure interoperability and adoption of the European Digital Identity Wallet (learn more at https://eudiwalletconsortium.org/)

EWC Payment Taskforce: led by Visa, this EWC workgroup is composed of Identity and Payment experts dedicated to writing the specifications of how the EUDI Wallet will be used for card and account payments, and experiment those specifications in live pilots (see Appendix A.1)

Holder: An entity that receives Verifiable Credentials (VCs) and has control over them to present them to the Verifiers as Verifiable Presentations (VP). The term **Holder** may be used alongside or, in place, of **User** in some situations.

International bank account number (IBAN): An internationally agreed upon system of identifying bank accounts across national borders to facilitate the communication and processing of cross-border transactions with a reduced risk of transcription errors.

Issuer: A Person Identification Data Provider issuing Person Identification Data (PID) or a (Qualified) Trust Service Provider issuing (Q)EAA. In the case of the EUDI Wallet there may be multiple Issuers for PID and (Q)EAA.

Merchant's Acquirer: A merchant's Payment Service Provider (e.g. a bank) that process debit or credit card payments on behalf of a merchant by sending payment transaction information to the card network for authorisation (i.e. for blocking of the cardholder's funds/payment to the merchant). Throughout this document, the term payee PSP is used instead.

Merchant/Payee: The recipient of the payment, which is generally a provider of goods or services (can also be a marketplace facilitating sales for various providers, such as Expedia), located anywhere in the world (but initially most likely mainly European located merchants). The Merchant is the one initiating a user's authentication request during a payment transaction.

Co-funded by the European Union

Payer/PSU (payment service user)/User: Holder of a EUDI Wallet and of a card or payment account from a European PSP, purchasing good or services on a merchant website or app who needs to be authenticated to pay for said purchase with her card.

Payment Initiation Service Provider (PISP): Third party that is harmonised to make payments on behalf of bank customers (users/payers) by initiating direct transfers to or from the payer's bank account using the bank (ASPSP)'s tools (APIs).

Payment Service Provider (PSP): A generic term to designate a European provider of payment services. In this document, whenever the term PSP is used it specifically (and only) refers to either:

- A Card-Based Payment Instrument Issuer or,
- An ASPSP (Account servicing payment service provider)

In laymen's terms, those entities are often referred to as "Bank", but they can be any type of organisation with appropriate licenses to provide the above-mentioned payment services.

A PSP can work on behalf of the payee (for example a merchant selling goods) or a payer (for example a consumer making a purchase). Therefore, this document refers to payee PSP (often called acquirer) and payer PSP, to indicate their role.

Person Identification Data (PID): A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

Person Identification Data (PID) Providers: trusted entities responsible for:

- verifying the identity of the EUDI Wallet User in compliance with LoA High requirements,
- issuing PID to the EUDI Wallet in a harmonised common format and
- making available information for Relying Parties to verify the validity of the PID.

Relying Party (RP): The PSP is the Relying Party during SCA. Relying parties, such as banks, must also accept the use of European Digital Identity Wallets for strong consumer authentication (SCA).

Qualified Electronic Attestation of Attributes (QEAA) providers: Issues an attestation to the user that their EUDI Wallet instance can be used for SCA, which is referred to as an "Payment Wallet attestation". QEAA Providers maintain an interface for requesting and providing QEAAs, including a mutual authentication interface with EUDI Wallet and potentially an interface towards Authentic Sources to verify attributes. QEAA Providers provide information or the location of the services that can be used to enquire about the validity status of the QEAAs, without having an ability to receive any information about the use of the attestations.

Strong Customer Authentication (SCA): Requires that the payer is authenticated through at least two factors, which must be independent from the other, from two of the three categories listed below.

- Something the payers know (knowledge factor, e.g. a PIN code)
- Something the payer has (possession factor, e.g. a mobile phone)
- Something the payer is (inherence factor, e.g. biometric)

Token Requestor Aggregator (TRA): A provider of payment token services to a merchant (not all merchants use such a provider – this is optional).

Token Service Provider (TSP): Responsible for the issuance and management of payment tokens. The TSP is an entity within the payments ecosystem that provides registered token requestors – for example the merchants holding the card credentials – with 'surrogate' PAN values, otherwise known as payment tokens. These payment tokens can only be used in specific domains such as a merchant's online website or a pre-defined channel like a mobile device.

Trusted List Provider (TLP): Verifies the status of a role in the EUDI Wallet ecosystem. It provides a registration service for an entity performing a particular role(s) and maintains a registry ("Trusted List") to enable third parties to access registration information. In this use case, the card issuer must check with a TLP that an EUDI Wallet provider and EUDI Wallet instance have a valid status on the Trusted List.

Verifiable Credential (VC): An Issuer-signed Credential whose integrity can be cryptographically verified. It can be any format used in the Issuer-Holder-Verifier Model.

EWC | Co-funded by the European Union

Verifiable Presentation (VP): A Holder-signed Credential whose authenticity can be cryptographically verified to provide Cryptographic Holder Binding.

1.6 Use cases

This document describes the following use cases:

- Registration for SCA: The user must register the EUDI Wallet for SCA with a PSP. This use case is a pre-condition for the other two use cases described in this document (Section 2).
- SCA for card-based transactions (Section 3).
- SCA for account-based transactions (Section 4).

1.7 Redirection methodology

Throughout this document there are references to redirections from the EUDI Wallet to a PSP app or merchant app and vice versa. This will be implemented with an Open ID common protocol handler described here: OpenID4VC High Assurance Interoperability Profile with SD-JWT VC - draft 00 .

The display objects defined here will be used to make it clear to the user to which app they are redirected. Specific profiles on how to implement redirection will be described in technical specifications to be published at a later stage.

EWC | Co-funded by the European Union

2.Registration of EUDI Wallet for SCA

Before an EUDI Wallet instance can be used to perform SCA during a transaction, it must be registered with the Payer's Payment Service Provider (PSP). The EUDI Wallet instance must provide several 'attestations' proving that the user, device, EUDI Wallet are eligible for SCA. In return, the EUDI Wallet instance obtains a Payment Wallet attestation from the PSP proving that it can be used for SCA.

Registration can be started with the following methods:

A. Using the Payer PSP app or website,
B. After EUDI Wallet installation, the EUDI Wallet offers to register for SCA with a PSP,
C. User selects the "register my EUDI Wallet instance to perform authentication for online purchase" menu in the EUDI Wallet,
D. Payer PSP sends push message to mobile device suggesting registering the EUDI Wallet for SCA,
E. After opening an account with a PSP using EUDI Wallet instance, the PSP suggests registering the EUDI Wallet to perform SCA for this account.

Please note that Method A must be supported by all EUDI Wallets. Support for Methods B to E is optional.

eIDAS2 regulation also mandates PSPs to propose the use of EUDI Wallets for online identification when accessing online/mobile banking applications[3], and this would also require a registration process. This chapter is about the registration of an EUDI Wallet as an SCA authentication method with the User's PSP. Synergies between the two processes to avoid double registration are not covered at this stage.

2.1 Pre-conditions

Prior to the registration process starting, with any methods, the following must be true:

1. The PSP must have been added to a Trusted List.
2. The EUDI Wallet solution must have been certified by an accredited public or private body designated by a Member State, must have been added to a Trusted List, and must have a "valid" status (i.e., cannot have a suspended status).
3. The user must already have installed an EUDI Wallet instance from a "valid" wallet solution from an EUDI Wallet provider present on the Trusted List. The EUDI Wallet instance must have a "valid" status. It must also be bound to a device possessed by the user e.g., mobile, tablet, security token, to act as a possession factor in the authentication process.

2.2 Actors

The following actors play a role in this use case:

- User
- Payer PSP: the party receiving the customer's request to register the EUDI Wallet instance to perform SCA or the party who can suggest to the customer that they should register one of the EUDI Wallet providers supported for this function. It is acting both as a (Q) EAA provider and a Relying Party (RP):
    - In its role as a (Q) EAA provider it is issuing an attestation to the user that their EUDI Wallet instance can be used for SCA. This attestation is referred to as a "Payment Wallet attestation".
    - In its role as Relying Party, the PSP is requesting attestations from the EUDI Wallet provider to determine whether the EUDI Wallet instance can be used for SCA. In the card payment scenario, the card issuer is the Relying Party (RP).

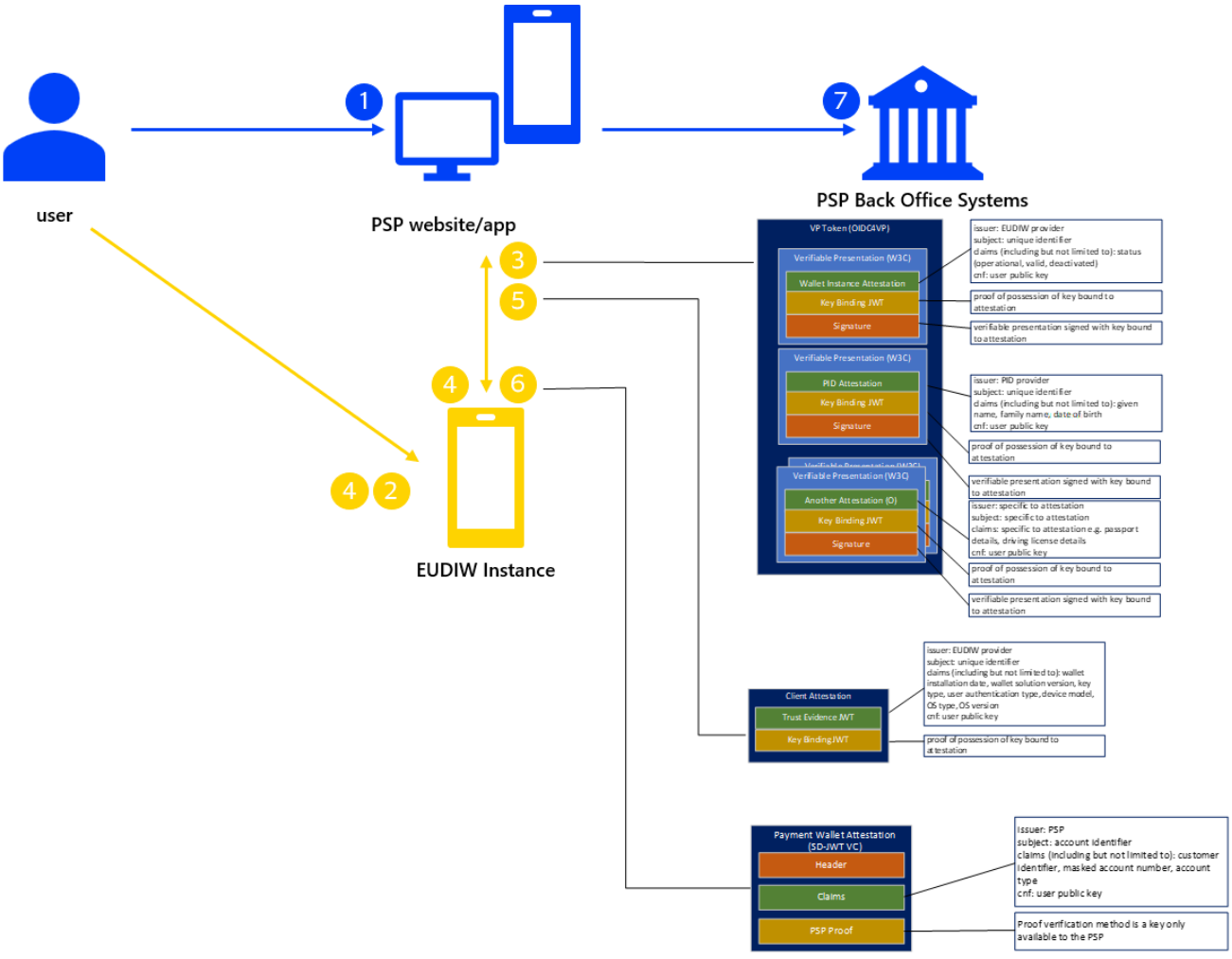
[3] *" […] to support the fulfilment of strong customer authentication requirements for online identification for the purposes of account login and of initiation of transactions in the field of payment services."* Recital (62) of eIDAS2 adopted regulation https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.pdf

EWC | Co-funded by the European Union

- Trusted List provider
- EUDI Wallet Instance
- EUDI Wallet Provider

2.3 High-level Registration flows

2.3.1 Flow for Registration Method A: Registration using PSP app or Web portal



1. The user is logged on to PSP app/portal. The user wishes to use their EUDIW to authenticate transactions for particular account(s). The user selects the accounts they would like to use the EUDIW as an authenticator for.

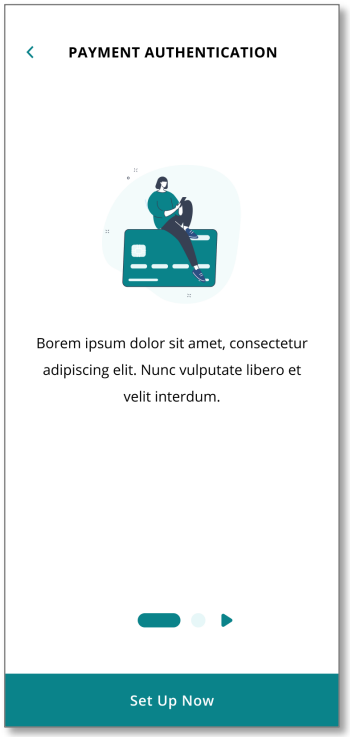
Steps 2 and 3 are optional

2. The PSP requires further information about the wallet holder perhaps to verify that the account holder is the wallet holder. They inform the user that they need to ensure that their wallet is secure. The PSP requests attestations from the EUDI Wallet instance about the user and validity of their EUDI Wallet instance by creating a presentation authorisation request which is displayed as a QR code (website) or deep link (app). The user scans the QR code using their EUDI Wallet instance or taps the deep link to open their EUDI Walley instance. The User authenticates to EUDI Wallet instance successfully.
3. The user confirms that they want to share the attestations requested with the PSP and the EUDI Wallet instance sends the verifiable presentation containing the requested attestations to the PSP, together with status of the EUDI Wallet instance. The PSP verifies the attestations and details of the EUDI Wallet instance.
4. The PSP generates a 'credential offer' that will allow the user to use their EUDI Wallet instance to facilitate SCA for the accounts selected. The PSP generates a transaction code (cross-device flow only) which is sent to the user over a separate channel. If the PSP has not performed steps 2 and 3 and the user is still in the PSP app / portal, they generate a QR code / deep link containing the credential offer which the user scans / taps to open their EUDIW instance and authenticates. Otherwise, the PSP sends the credential offer to the EUDI Wallet instance in response to step 3 and the user remains within their EUDIW instance.
5. The EUDI Wallet instance requests the credential (payment wallet attestation) from the PSP, passing proof of the user (public key) and the transaction code which it requests from the user (cross-device flow only). It passes further information on the technical capabilities of the EUDI Wallet instance
6. The PSP validates the proof of public key, transaction code (cross-device flow only) and generates the payment wallet attestation, including the public key of the user, and returns it to the EUDI Wallet instance.
7. The PSP app/portal sends the payment wallet attestation and public key to their back-office system to store and make accessible to their ACS and/ or other systems to use during account authentication.

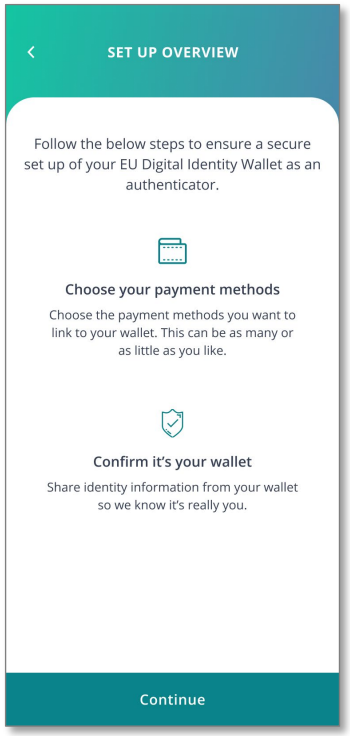
2.3.1.1 User experience example – App to App

Below an example of the user experience for this flow:

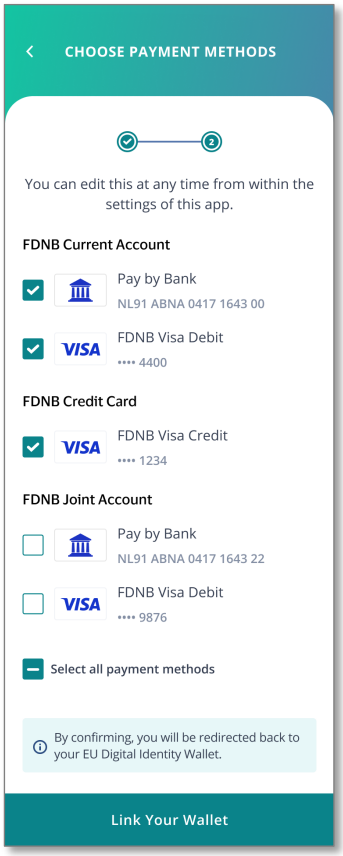
1) User is in PSP app and selects option to set up EUDI Wallet as authenticator.



2) App displays steps. User selects Continue.

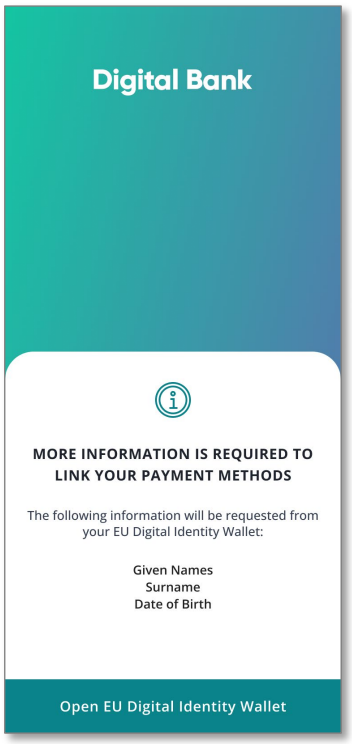


3) PSP app displays list of cards/accounts which can be linked to the EUDI Wallet. User selects.

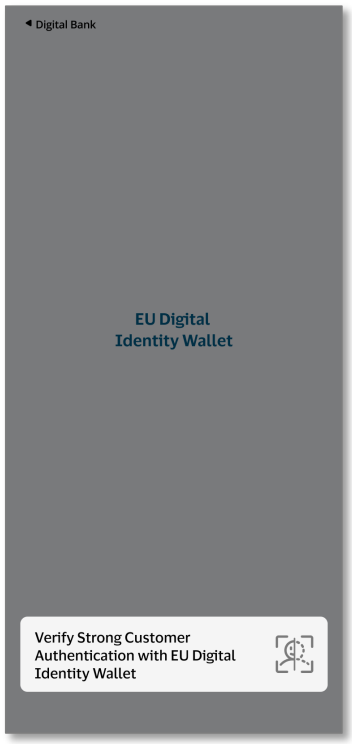


EWC | Co-funded by the European Union

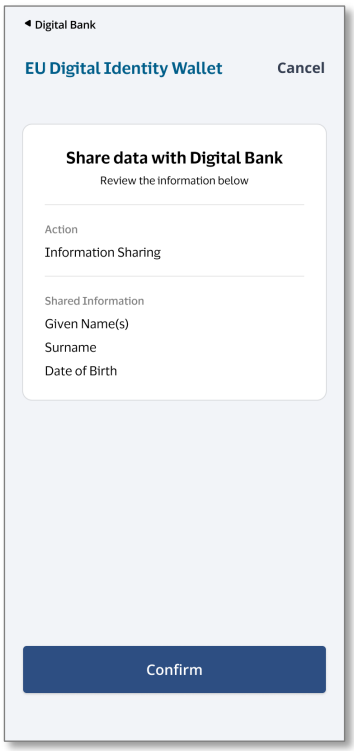
4) PSP app displays any information required from the user to verify their EUDI Wallet.



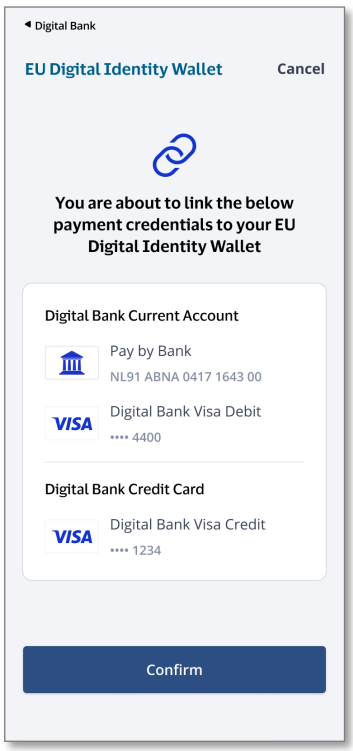
5) User authenticates to EUDI Wallet for the activity of sharing information.



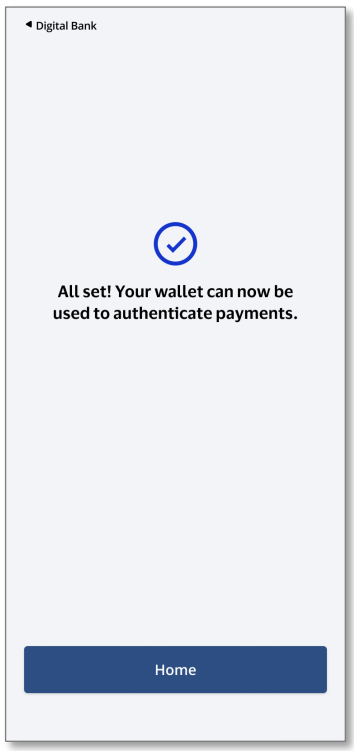
6) EUDI Wallet asks user to share personal information with PSP app. User confirms.



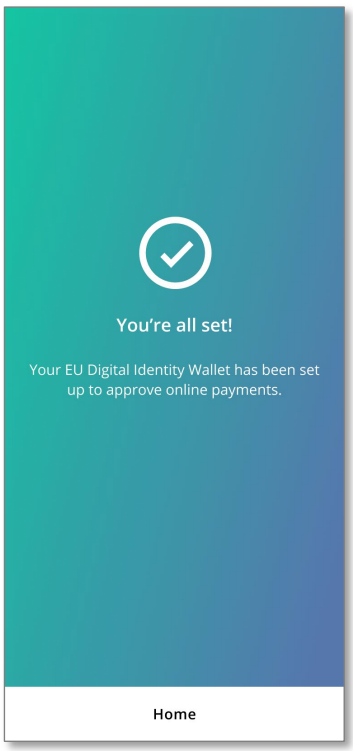
7) EUDI Wallet asks the user to confirm the payment methods being linked.



8) EUDI Wallet displays that it is successfully registered for SCA.



9) The user can manually redirect to the PSP app which also displays confirmation.



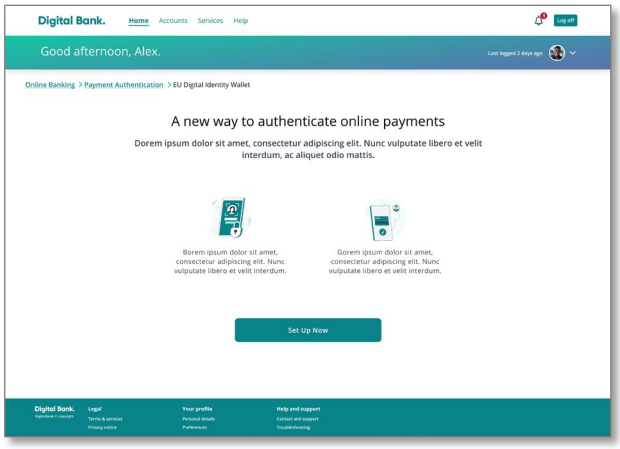
Co-funded by the European Union

Note: The PSP may, e.g. around step 3, additionally incorporate an SCA using existing functionality to further secure the activity of linking the wallet to the cards/accounts.

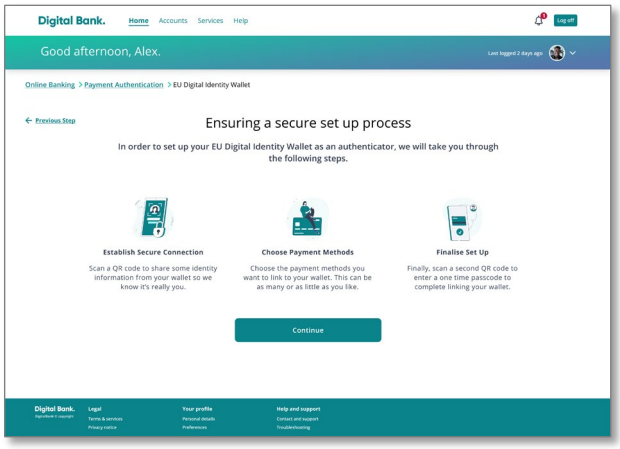
2.3.1.2 User experience example – Browser to app

If the PSP Web portal is used (for example on a desktop computer) instead of the PSP mobile app, the flow is similar with a few differences. Instead of a deep link, portal displays QR code to open EUDI Wallet.

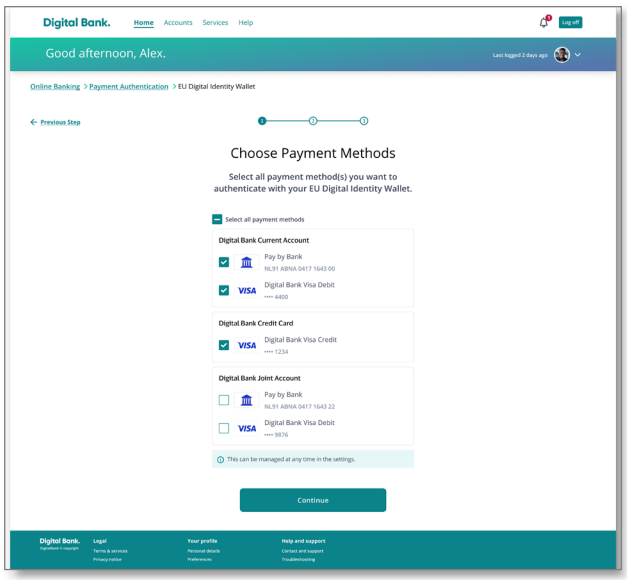
1) In PSP portal, user selects option to register EUDI Wallet for SCA.



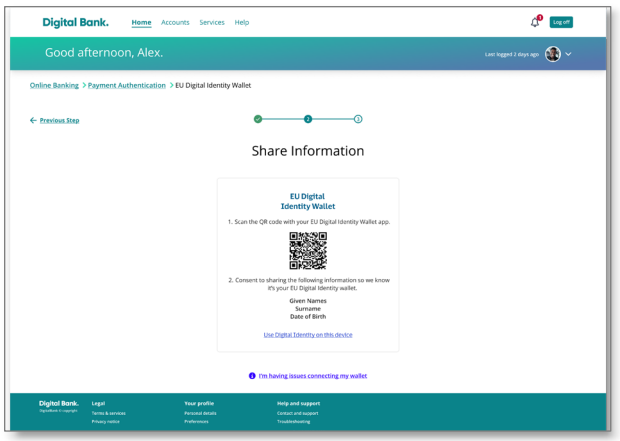
2) Portal displays steps. User clicks Continue.



3) PSP Portal displays cards for which EUDI Wallet can be registered. User makes selection and clicks Continue.



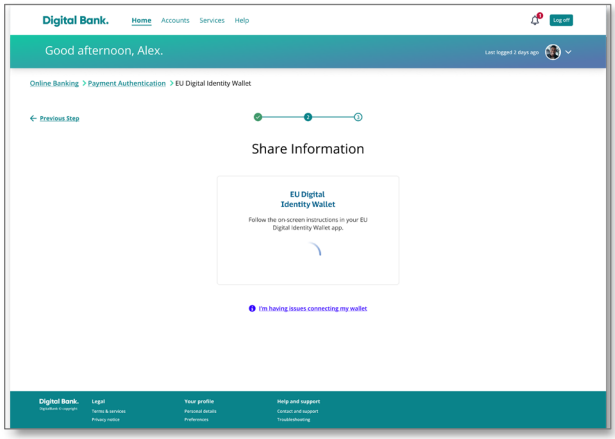
4) PSP Portal displays QR code which will launch EUDI Wallet and requests personal information.



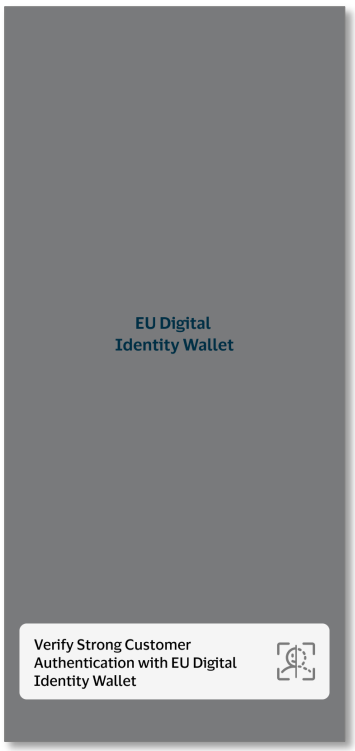
Co-funded by the European Union

5) User opens EUDI Wallet and scans QR code.

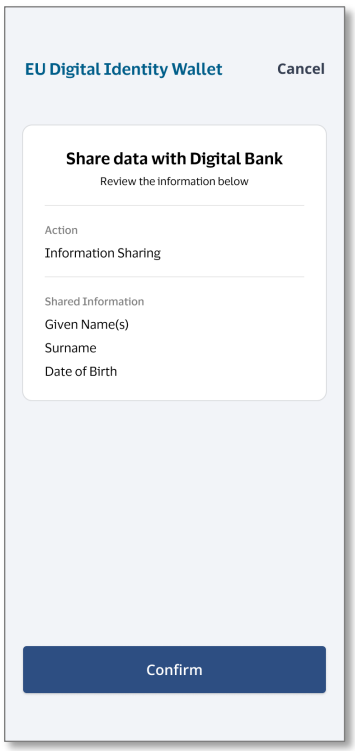
6) PSP Portal sets up secure connection with EUDI Wallet.



7) User authenticates to EUDI Wallet for the activity of sharing information.

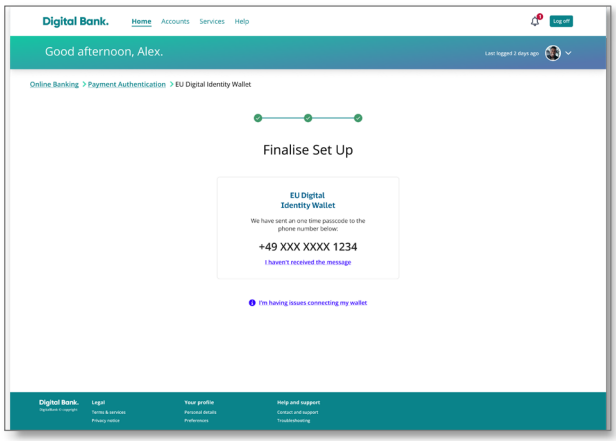


8) EUDI Wallet asks user to share information with PSP portal. User confirms.

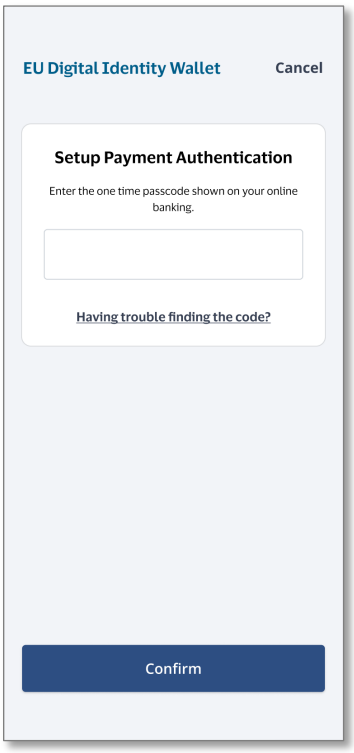


Co-funded by the European Union

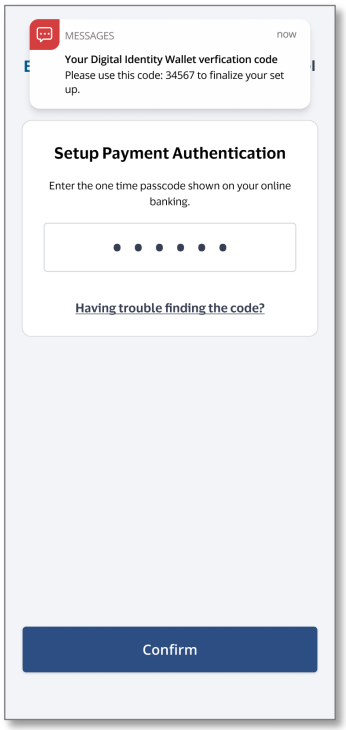
9) PSP portal displays a masked phone number where a one-time passcode (OTP) has been sent which will finalise registration of EUDI Wallet for SCA.



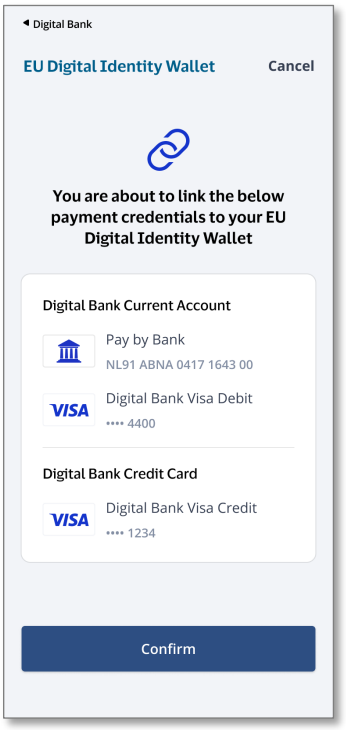
10) EUDI Wallet displays option to enter OTP.



11) User receives and enters their OTP in EUDI Wallet.

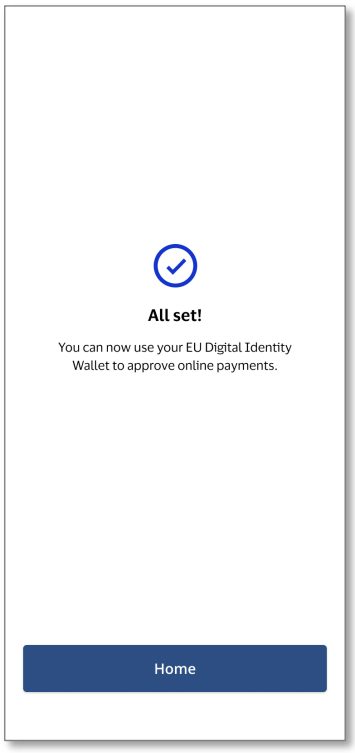


12) EUDI Wallet asks the user to confirm the payment methods being linked.

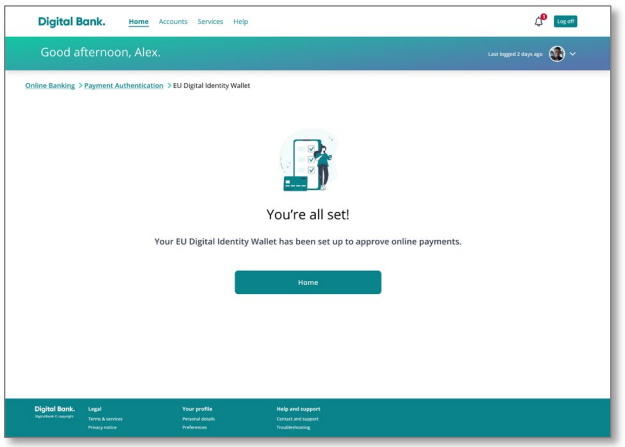


Co-funded by the European Union

13) EUDI Wallet displays confirmation message.

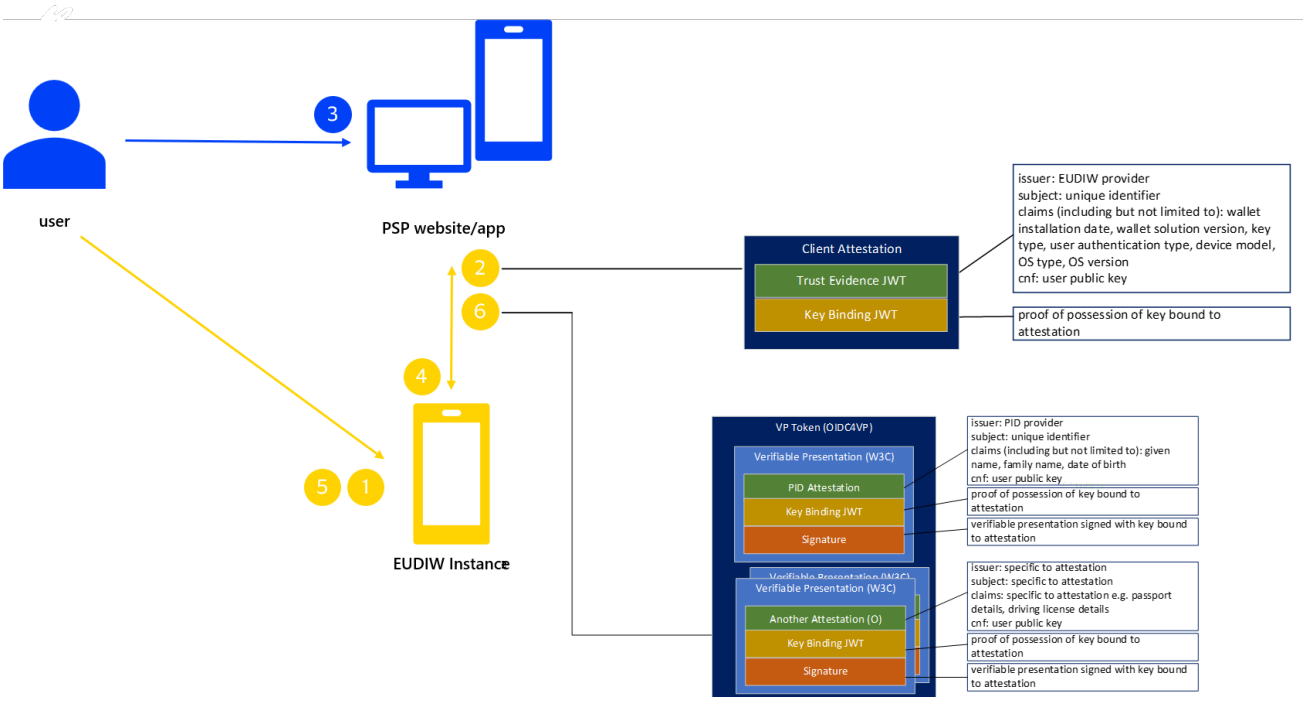


14) PSP Portal also displays confirmation message.



Note: The PSP may, e.g. around step 3, additionally incorporate an SCA using existing functionality to further secure the activity of linking the wallet to the cards/accounts.

2.3.2 Flow for Registration Method B: Registration using EUDI Wallet after setup



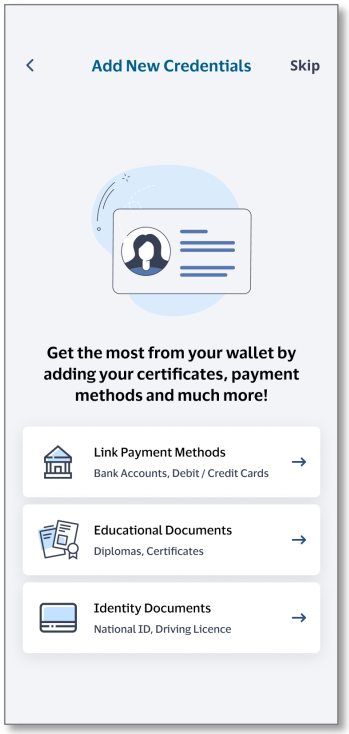
1. The user completes onboarding onto their EUDI Wallet instance and chooses to link it to their PSP account. The user is a presented a list of PSPs on the Trusted List and selects their PSP
2. The EUDI wallet instance sends an authorisation request to the PSP, containing details on the technical capabilities of the wallet instance and its validity; to request the credential (payment wallet attestation). The PSP confirms that the wallet provider is on the trusted list, the wallet solution is valid, the wallet instance is valid and that the EUDI wallet instance can be used as an authenticator. The EUDI wallet instance sends the authorisation request by either using a deep link to open the user's PSP app, or launching the default browser on the user's device that navigates to the PSP portal.
3. The user authenticates to the PSP. The user then selects the accounts for which they wish to the use the EUDI wallet instance as an authenticator.
4. The PSP generates an authorisation response that is sent to the redirect URI specified by the EUDI wallet instance in the authorisation request. The user is automatically switched to the EUDI wallet instance when the PSP calls the redirect URI.
5. The user may or may not need to reauthenticate into the EUDI wallet instance.
6. The PSP may have issued an authorisation code at this stage but if not, it may request more about details about the user. In this case the EUDI Wallet instance, with consent from the user, will send a verifiable presentation containing the information requested. The PSP will validate it and then issue the authentication code.

Remaining steps as per method A step 5

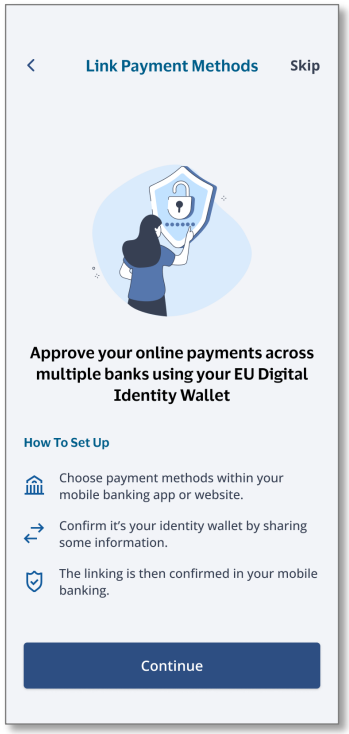
2.3.2.1 User experience example – App to app

Below an example of the user experience for this flow:

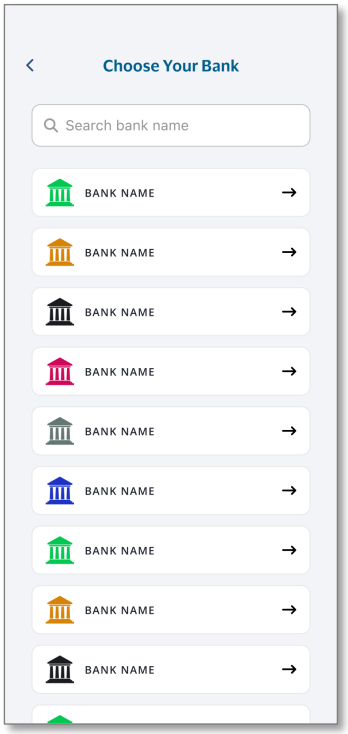
1) After EUDI Wallet installation, EU DI Wallet triggers the user to link payment methods. User selects this option.



2) EUDI Wallet displays the steps in the process. User taps Continue.

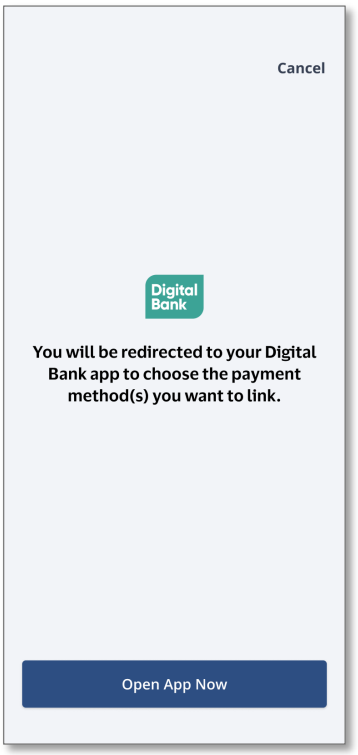


3) User selects their PSP.

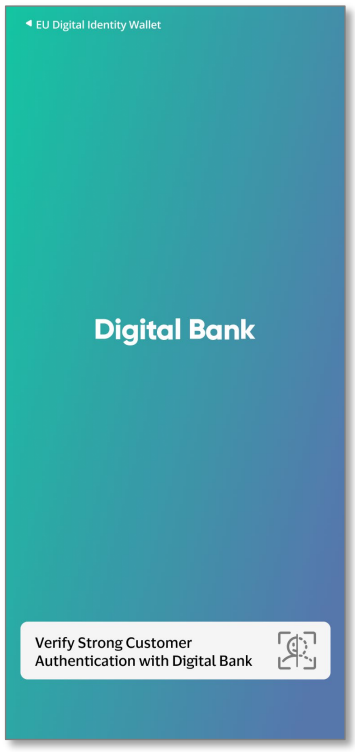


EWC | Co-funded by the European Union

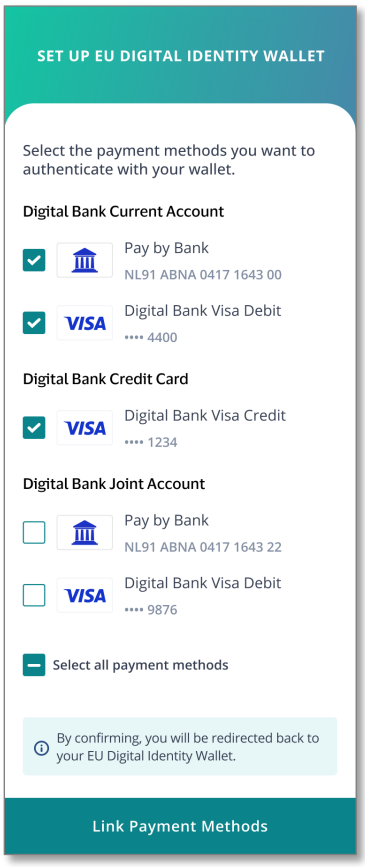
4) User is redirected to the PSP app to choose the payment methods they want to register for SCA.



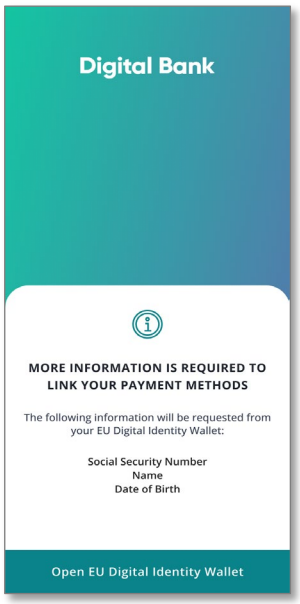
5) User authenticates to the PSP app.



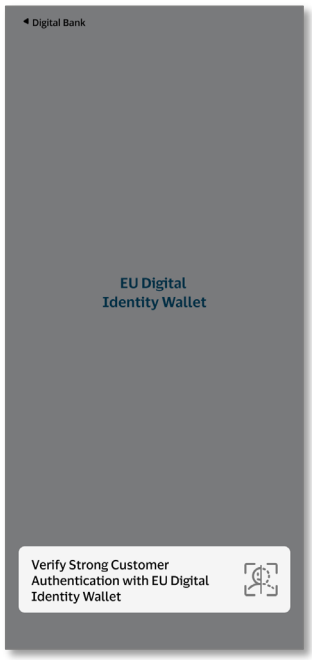
6) User selects accounts they wish to register for SCA.



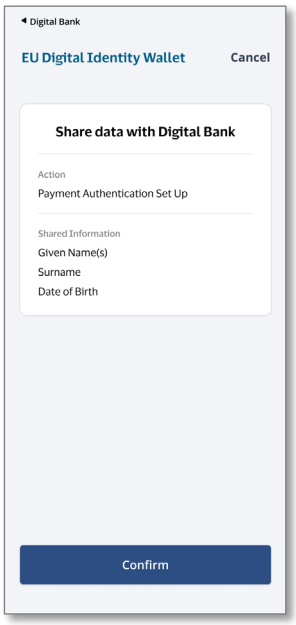
7) User is informed that further information is needed before registration can complete and they requested to return to their wallet



8) User authenticates to EUDI Wallet for the activity of sharing information.

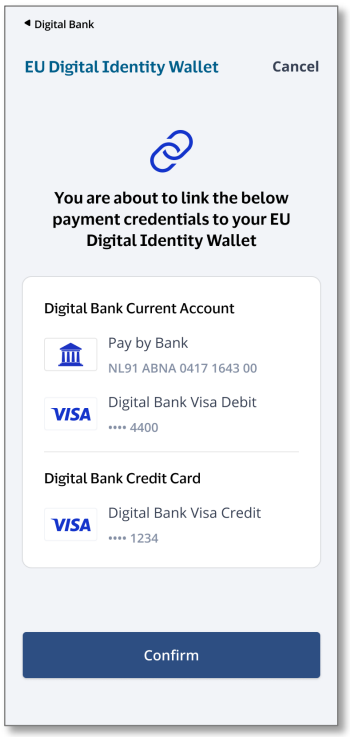


9) EUDI Wallet requests consent from the user to share additional information with the PSP.

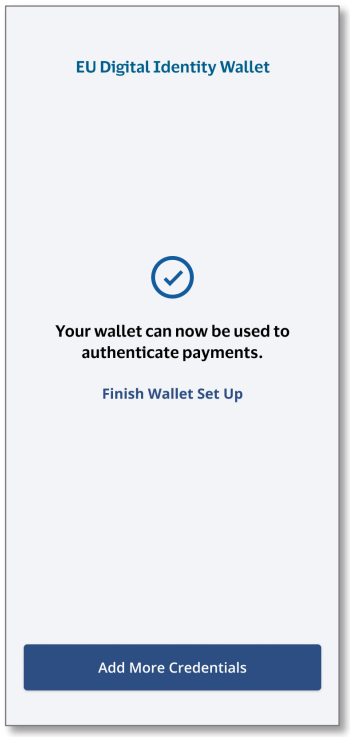


Co-funded by the European Union

11) EUDI Wallet asks the user to confirm the payment methods being linked.

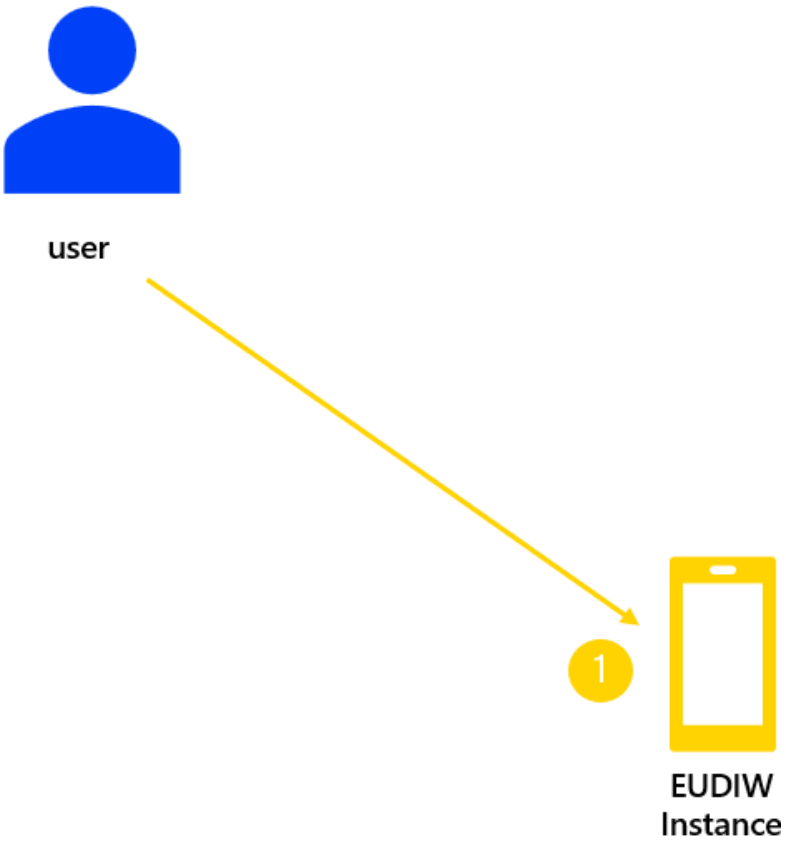


11) EUDI Wallet displays confirmation message.



Co-funded by the European Union

2.3.3 Flow for Registration Method C: Registration using EUDI Wallet using menu

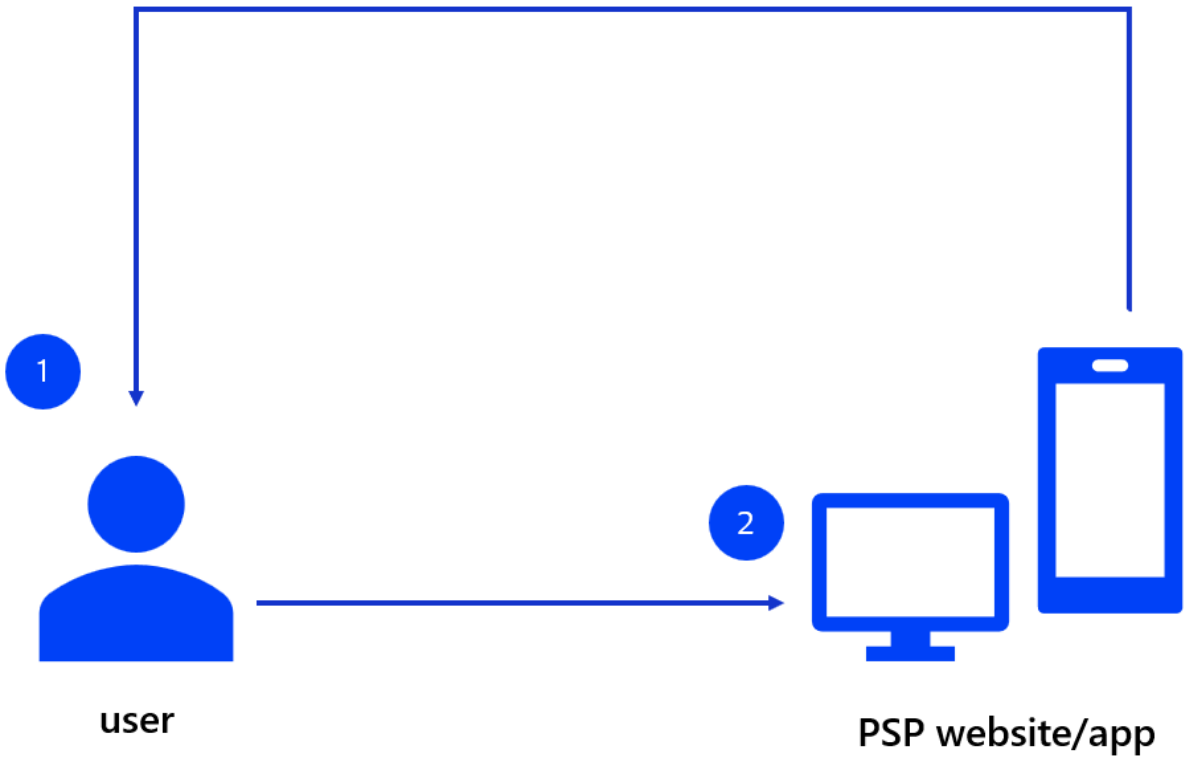


1 The user selects a PSP from the Trusted List to link their EUDI Wallet to.

Remaining steps as per method B step 2

Co-funded by the European Union

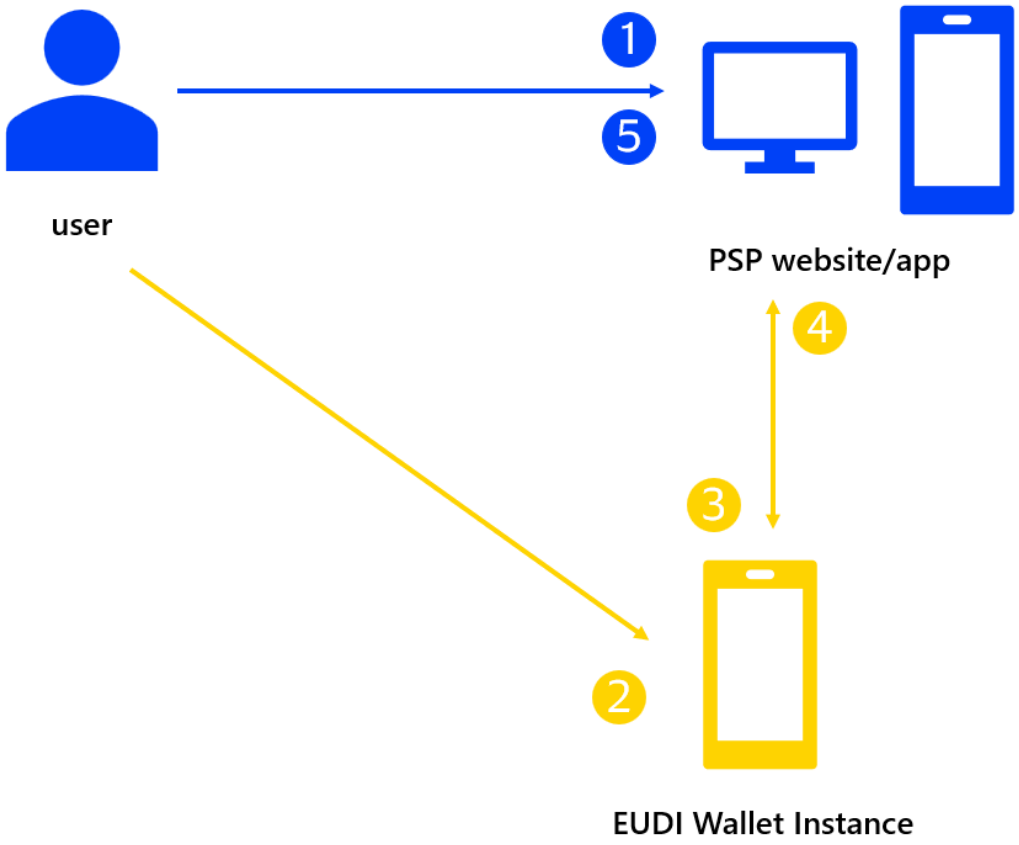
2.3.4 Flow for Registration Method D: Registration after receiving notification from PSP



1	The PSP notifies the user that they can use their EUDI Wallet instance to authenticate payments against their account.
2	User logs into PSP app/portal (if not already in) and selects the option to enable an EUDI Wallet for authentication.
	Remaining steps as per method A step 1

EWC | Co-funded by the European Union

2.3.5 Flow for Registration Method E: Registration after using EUDI Wallet to open account



1. The user selects the EUDI Wallet that they wish to use to onboard to the PSP with
2. The PSP requests a verifiable presentation from the EUDI Wallet instance containing attestations needed for account opening by generating a QR code (website) or deep link (app) which launches the user's EUDI Wallet instance, when they scan the QR code or tap the deep link.
3. The user scans the QR code using their EUDI Wallet instance or taps the deep link. User authenticates to EUDI Wallet instance successfully.
4. The user confirms that they wish to share the attestations requested with the PSP and the EUDI Wallet instance returns the verifiable presentation containing these attestations to a URL provided by the PSP. The user is asked to return to their PSP portal / app.
5. The user confirms that they want to use their EUDI Wallet instance to authenticate payments against their account.

Remaining steps as per method A step 4

2.4 Responsibilities per actor

2.4.1 EUDI Wallet

To enable SCA registration using **Registration Method A**, the EUDI Wallet must be able to:

- Be launched by scanning a QR code or tapping a deep link.
- Receive a request for a verifiable presentation from the PSP embedded in a deep link or QR code.
- Return a verifiable presentation containing the attestations requested by the PSP, which it will subsequently use to verify the user is the account/card holder. If requested, these as a minimum will include a PID

EWC | Co-funded by the European Union

attestation that is issued by a PID provider. This will have a PID identifier as a subject and will contain the following claims (but not limited to): first name, last name, and date of birth.

- Provide the user with an opportunity to consent to sharing the above information with the PSP.
- Provide the PSP with the Trust Evidence JWT when it is requested.
- Receive an offer from the PSP to fetch a Payment Wallet attestation.
- Accept a PIN entered by the user when the user is accessing the PSP portal / app on a separate device to that which the EUDI Wallet Instance has been installed upon (cross-device flow).
- Request the Payment Wallet attestation from the PSP by passing the PIN (cross device flow only), the public key of the user and proof that the user possesses the public key.

Additionally, if **Registration Method B** is supported, EUDI Wallet must be able to:

- Present the user with a list of PSPs on the Trusted List.
- Send a request to the PSP to obtain a Payment Wallet attestation.
- Redirect the user to the PSP website, or to the PSP app by opening a deep link.

Additionally, if **Registration Method C** is supported, the EUDI Wallet must have:

- A menu option, for example to “register your EUDI Wallet to perform authentication during online purchases”.

Methods D and E don’t have any additional requirements for the EUDI Wallet.

2.4.2 PSP

To enable registration for SCA via registration **Method A**, the PSP app/Web portal must be able to:

- Trigger the user to enable their EUDI Wallet for SCA.
- Have the user select the accounts they wish to use the EUDI Wallet for SCA. As specified in eIDAS II Recital 62, the ASPSP ***should*** ensure that at least one IBAN is recorded in the EUDIW during the registration to support the fulfilment of SCA requirements for online identification for the purpose of the initiation of transactions.
- Receive the Trust Evidence JWT, a short-lived object that contains the combined set of claims in both the “WTE” and “WIA” as per the ARF, from the EUDI Wallet instance and validate that the Wallet Provider is on the Trusted List.
- Request a verifiable presentation containing the required attestations from the EUDI Wallet instance. The PSP app/portal must trigger the user to switch to EUDI Wallet instance by:
- generating a QR code that the user can scan,
- displaying a deep link.
- Validate the attestations in the verifiable presentation.
- Validate the user is indeed the same person as the account/card holder by using the attestations returned from the EUDI Wallet instance.
- Determine from the attestations received and the Trust Evidence JWT whether the EUDI Wallet instance can be used as authenticator and if it can send an offer to the EUDI Wallet instance of receiving a Payment Wallet attestation.
- Generate a PIN that the user can use to claim the offer in the EUDI Wallet instance (cross-device flow only).
- Receive the request for a Payment Wallet attestation and validate that it is linked to the verifiable presentation that was provided previously. Validate the proof of public key sent in the request.
- Generate the Payment Wallet attestation and embed the public key sent in the request, before returning it to the EUDI Wallet instance.

EWC | Co-funded by the European Union

- Store and share the attestations, Wallet Trust Evidence and Wallet Instance Attestation received from the EUDI Wallet instance.

Additionally, if **Method B** is supported, the PSP app/portal must be able to respond to a request by the EUDI Wallet instance for a Payment Wallet attestation by:

- Asking the user to confirm for which payment account(s)/card(s) they wish to use their EUDI Wallet instance as an authenticator.
- After confirmation has been given, redirecting the user to the EUDI Wallet, by opening a deep link to the EUDI Wallet instance.

Methods C. D and E don't have any additional requirements for the EUDI Wallet.

3.SCA for card-based transactions

This section covers using EUDI Wallet for SCA during card-based payments (the user enters card details or selects a card that has already been stored with merchant). Alternative scenarios are account and wallet payments.

A user's card details (also called card credentials) can take two different formats:

- a Primary Account Number, or PAN, which is the "long" number (usually 16 digits) written on a payment card, or
- a Payment Token, which is a unique identifier generated by a card network as a proxy for the PAN and that can be used (as an option) by merchant or their payment service providers to store the card number in their system for future use. This provides enhanced security.

Note that a payment card can be physical (e.g. a traditional plastic card) or virtual only (a digital number).

The technology used to support the authentication process will depend on the type of credentials used in the transaction:

- If a PAN is used, the EMV 3DS protocol/technology is used in the authentication process. The authentication data is captured by the PSP (**Method A**).
- If a Payment Token is used, the card network system's Token Service Provider (TSP) can be used in the authentication process without the use for EMV 3DS (**Method C**).

The PSP is responsible to ensure SCA is completed. However, there is market demand for merchants to remain in control of the user experience during a purchase flow. The payment industry is therefore starting to support new flows that enable merchants to capture the authentication data for final validation by the PSP. This is **Method B.** Here, usually a PAN is used, but it is also possible (but less likely) that a Payment Token is used.

3.1 Pre-conditions

The following pre-conditions apply:

1. The user has entered the payment card number on the merchant web site or app or selected to pay with a card already stored on file with the merchant.
2. Before the EUDI Wallet can be used to authenticate a payment transaction, it must be registered for strong authentication (SCA) with the user's payment card issuer (Payment Service Provider – PSP). This process is described in section 2 of this document.

If any of these pre-conditions are not met, the process cannot start.

3.2 Actors

The following actors play a role in this use case:

- User
- Merchant
- Payer PSP (role: Relying Party)
- Payee PSP (merchant's acquirer)
- Card Network
- Card Network Directory Server (DS)
- ACS (Access Control Server)
- EUDI Wallet
- Token Service Provider

EWC | Co-funded by the European Union

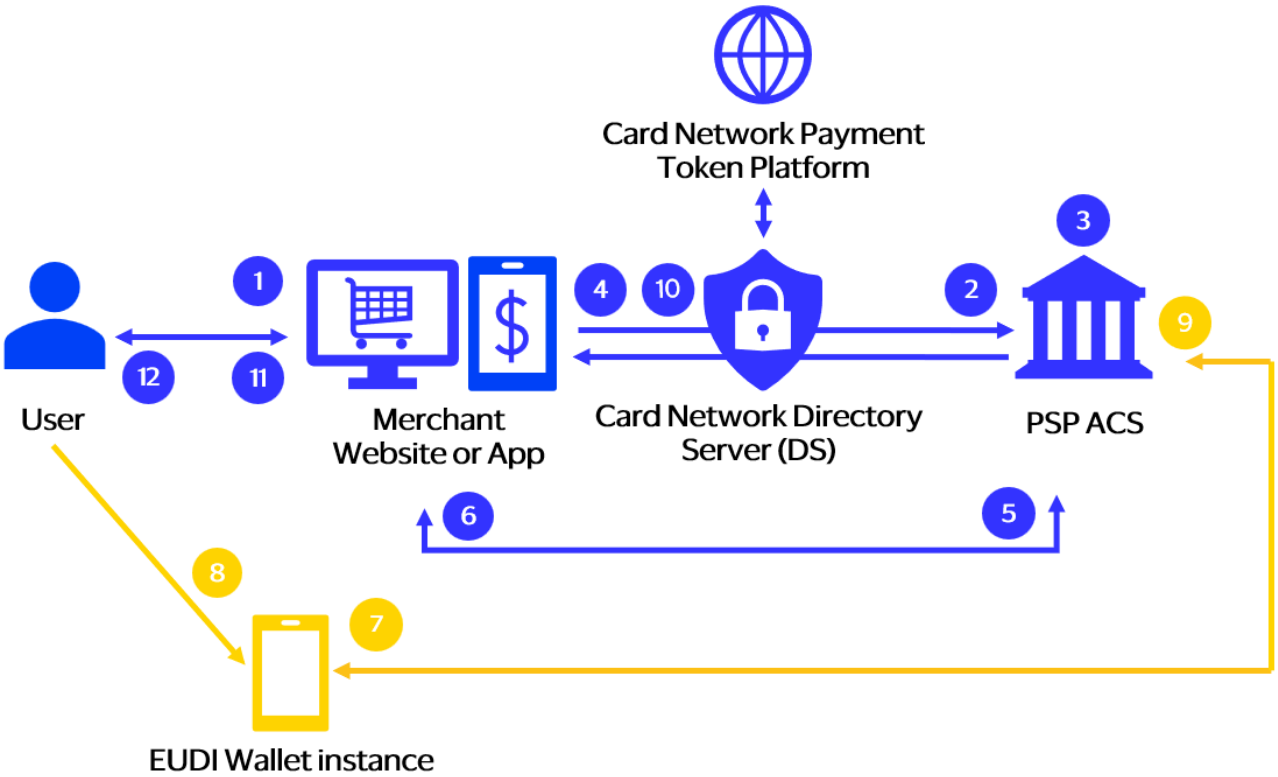
- Token Aggregator
- Trusted List Provider

3.3 High-level SCA Flows

3.3.1 Method A: Authentication data captured by PSP – Out of Band Authentication with EMV 3DS

The card issuer authenticates the user by receiving, from the merchant, the authentication request with the payment credential in the form of a PAN or payment token via an authentication technology named EMV 3DS. The card issuer will then connect to the EUDI Wallet with a process called out of band (OOB) authentication to use it for authenticating the user for this transaction. This flow variant is generally well-known in the ecosystem and already used by card issuers, either in conjunction with their own authenticator/online banking apps or in conjunction with market-wide solutions like e.g. Bank ID in the Nordics. Many card issuers in markets where there is no existing market-wide identity app and where authentication failure is high due to lack of a seamless way to authenticate would benefit from the availability of a standard to authenticate with the EUDI Wallet.

This method applies to both browser and app. Some messaging details/steps may vary depending on which one is used.



EWC | Co-funded by the European Union

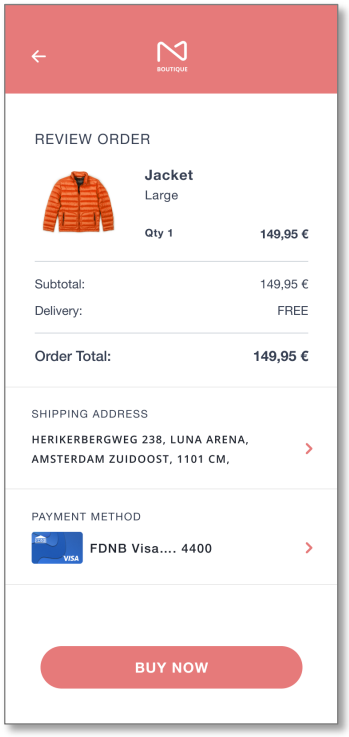
1. Consumer purchases goods and provides payment credentials (or confirms which "stored" credential to use).
2. Merchant sends authentication request to the PSP ACS via the appropriate card network DS. If a token was used the DS calls out the network token platform to detokenize and pass as a PAN to the ACS.
3. PSP ACS approves/declines/challenges authentication request (based on PSP risk policy). This diagram describes a challenge.
4. PSP ACS sends response via the appropriate card network DS to Merchant with the intent to challenge.
5. Merchant sends a request to the PSP ACS to initiate the challenge.
6. PSP ACS uses the PAN to determine that consumer uses EUDI Wallet and in a merchant browser scenario returns a page displaying a QR code that the user must scan to open their EUDI Wallet. Alternatively, in the browser scenario, the user must have been sent a push notification requesting they open their EUDI Wallet. If the user is in a merchant app scenario, they will be automatically switched to their EUDI Wallet.
7. PSP ACS requests the Payment Wallet attestation linked to the PAN which was placed in the EUDI Wallet at registration and the Wallet instance attestation. It passes the transaction details and the masked card number to the EUDI Wallet. The EUDI Wallet is invoked on consumer device (or has readiness to be invoked by the consumer).
8. The consumer authenticates into the EUDI Wallet instance. The EUDI Wallet instance asks the user to confirm sharing of the Payment Wallet attestation and Wallet instance attestation for the purposes of authenticating the transaction details shown. Consumer confirms sharing for this purpose.
9. EUDI Wallet provides the authentication data (Payment Wallet attestation, Wallet Instance attestation) back to the PSP ACS.
10. PSP or their ACS validates the authentication data and the ACS returns the results of the authentication back via the appropriate card network DS to Merchant.
11. EUDI Wallet instance redirects consumer to Merchant web site or app.
12. Merchant confirms authentication success to EUDI Wallet instance, which displays it to cardholder.

    Merchant must then proceed to authorisation flow (not covered in this flow).

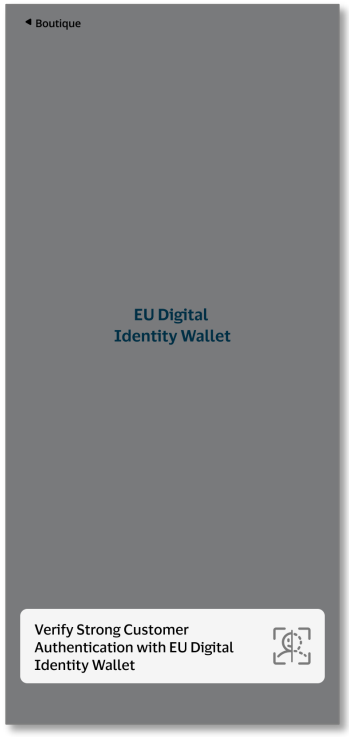
3.3.1.1 User experience example – App to App

Below an example of the user experience for this flow:

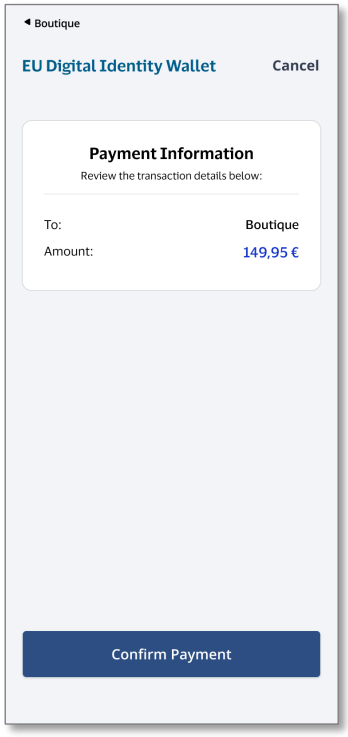
1) Using merchant app, user makes purchase using registered card.



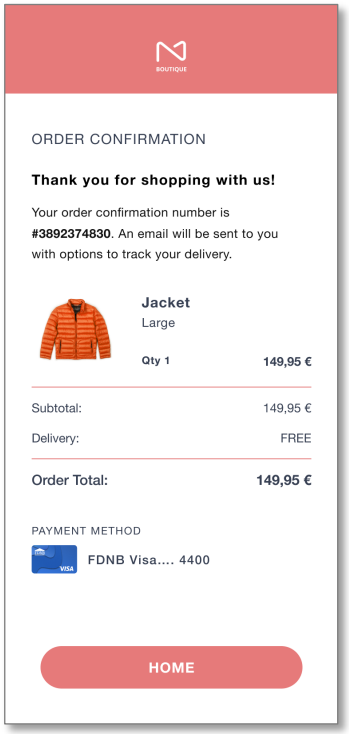
2) User authenticates to EUDI Wallet for the activity of payment confirmation.



3) User confirms payment.



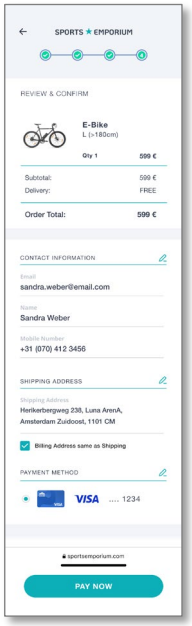
4) Merchant app confirms successful transaction.



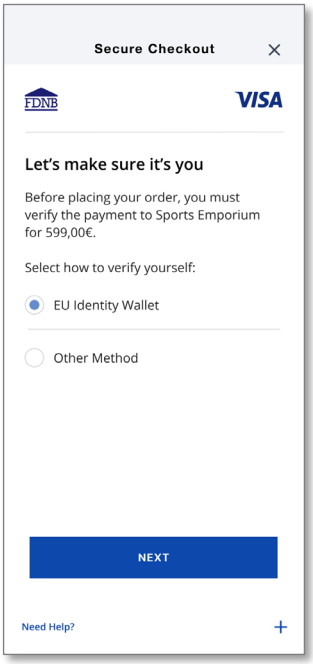
3.3.1.2 User experience example – mobile browser to app

Below an example of the user experience for this flow:

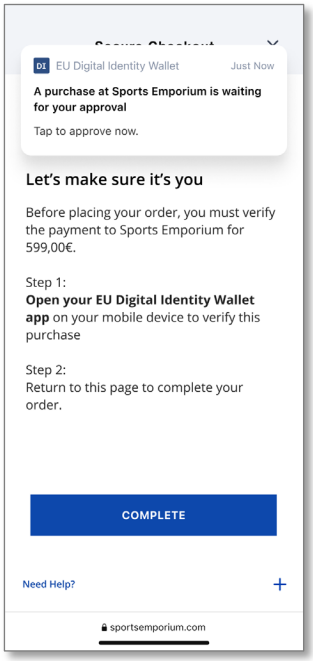
1) User makes purchase using ecom Web portal with mobile browser.



2) PSP suggests using registered EUDI Wallet for SCA.



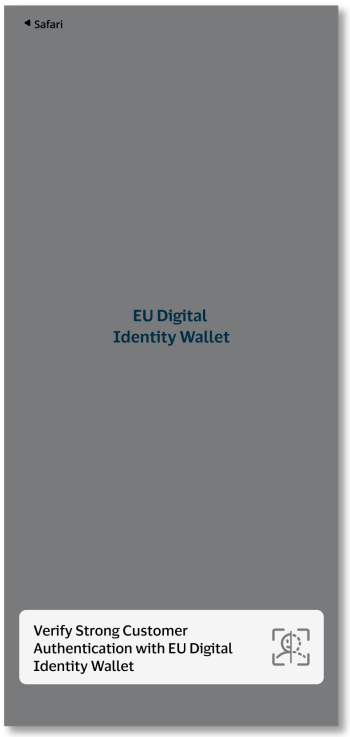
3) PSP sends push notification to EUDI Wallet. User taps to open EUDI Wallet.

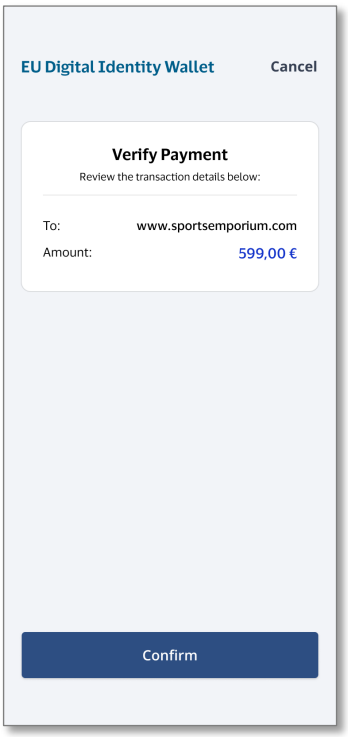


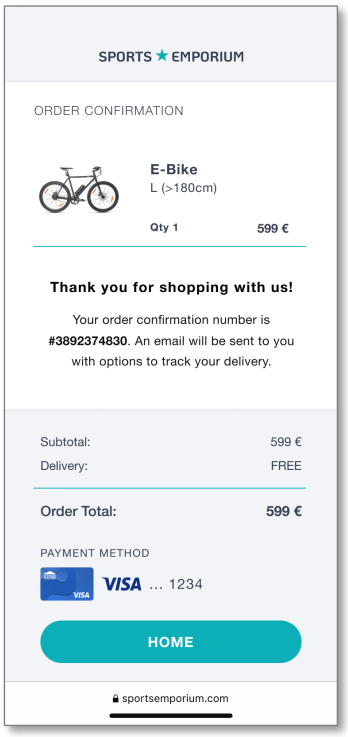
4) User authenticates to EUDI Wallet for the activity of payment confirmation.

5) User confirms payment.

6) Ecom portal shows successful transaction.





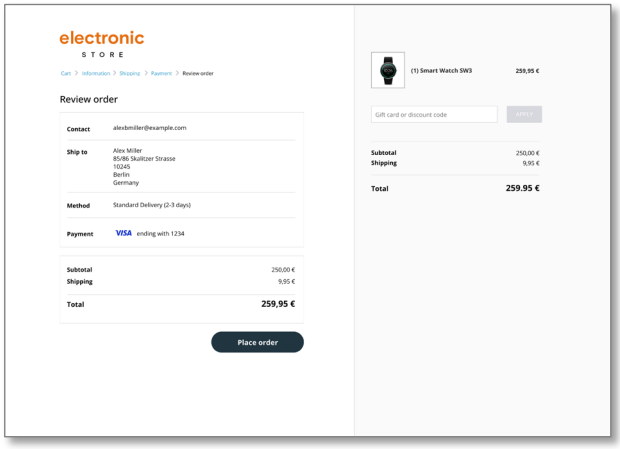


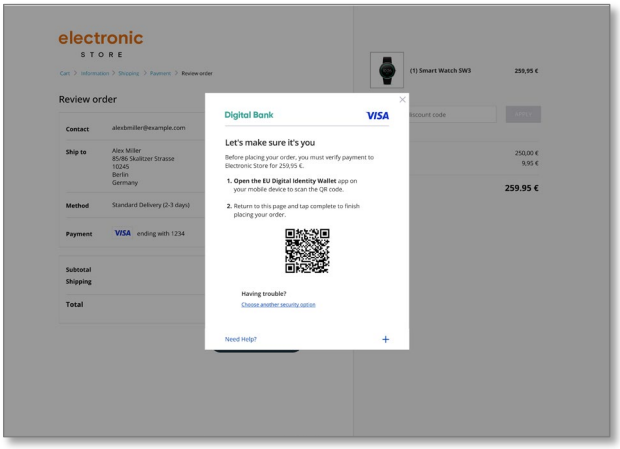
3.3.1.3 User experience example – desktop browser to app

Below an example of the user experience for this flow:

1) User makes purchase on ecom Web portal using desktop browser. Merchant has card details stored.

2) Merchant portal links to PSP, which displays QR code to scan with EUDI Wallet.

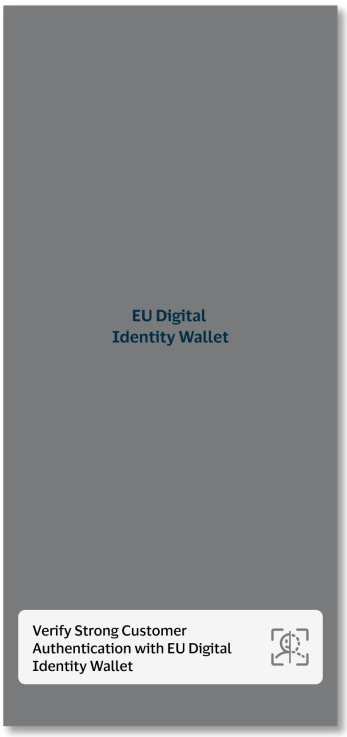




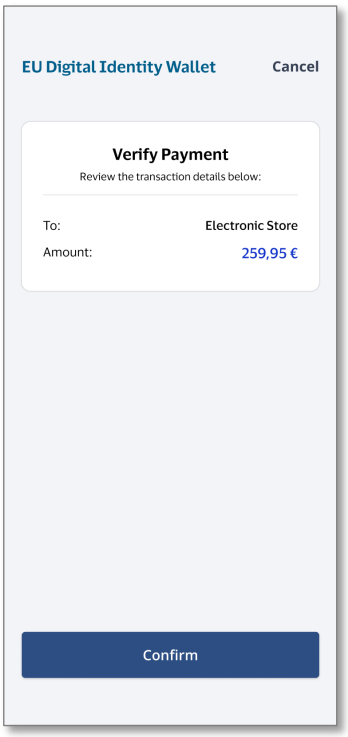
EWC | Co-funded by the European Union

3) User opens EUDI Wallet and scans QR code.

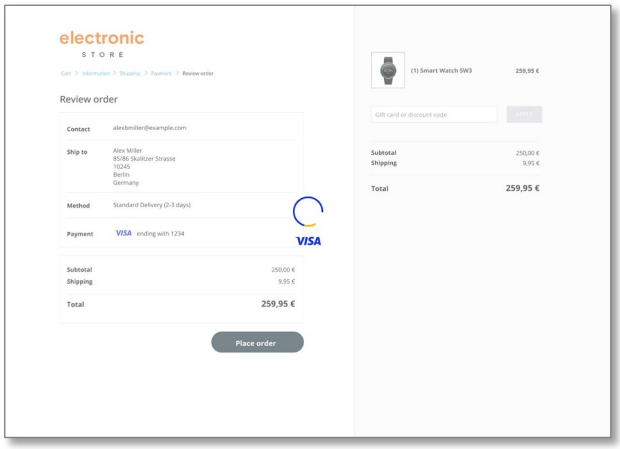
4) User authenticates to EUDI Wallet for the activity of payment confirmation.



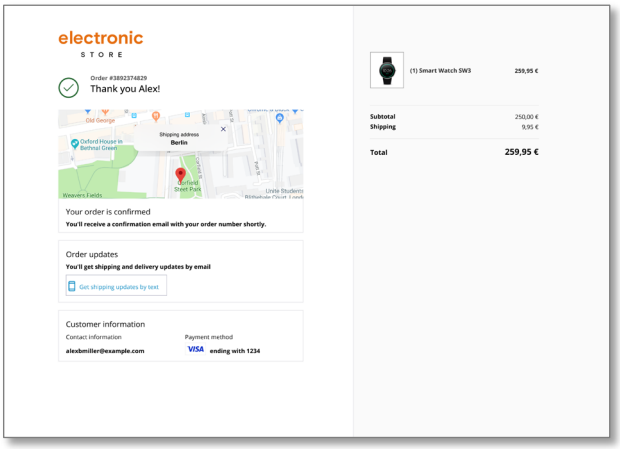
5) EUDI Wallet displays transaction details. User confirms.



6) Merchant portal displays PSP is processing transaction.



7) Merchant portal displays successful transaction.



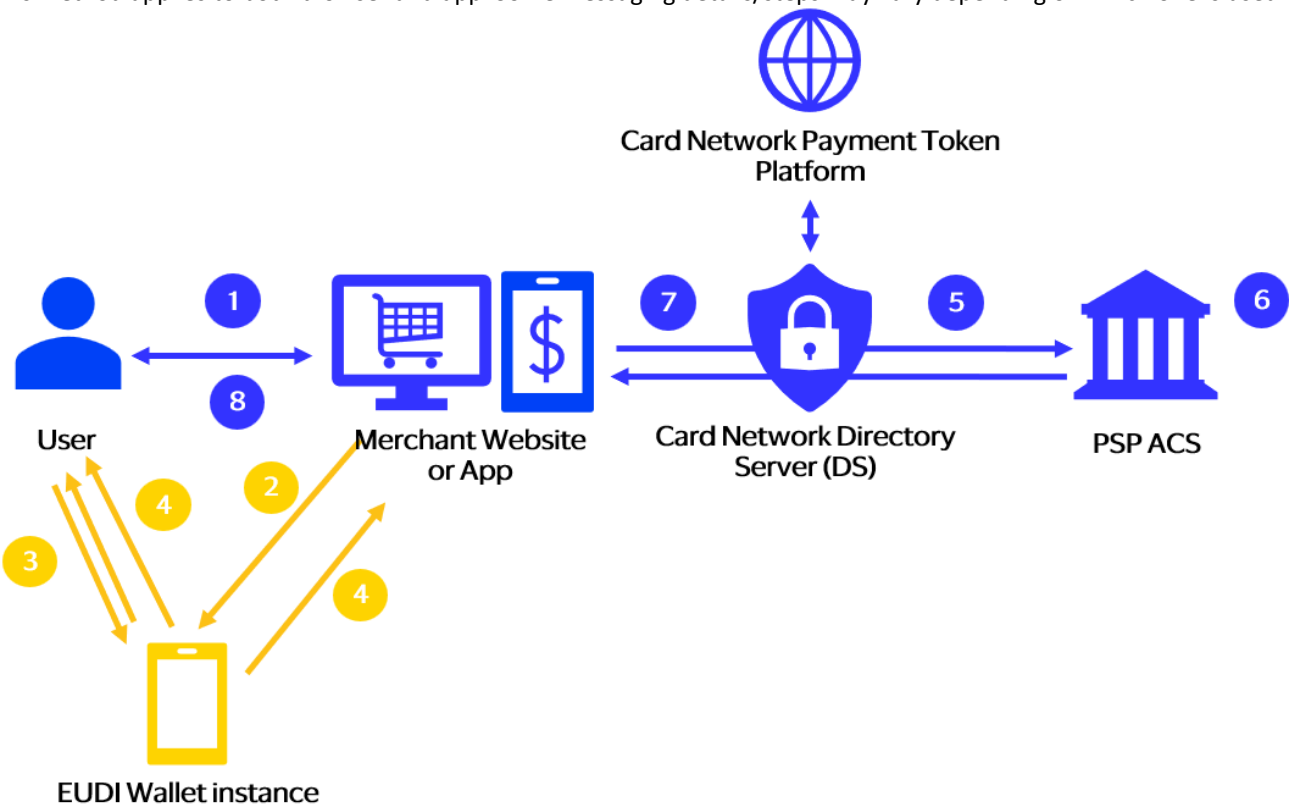
3.3.2 Method B: merchant-captured authentication data and EMV 3DS

As opposed to Method A, in this method the merchant interacts with the wallet. The authentication data is then relayed to the bank via the 3DS protocol. The bank inspects the data and returns an authentication response, which enables the merchant to proceed to payment authorization.

Whilst this method brings more requirements for the merchant to be able to interact with and process data from the wallet, it enables the merchant to ask for other attestations in parallel to the payment authentication. This way, the merchant could e.g. ask for an age verification or for the user's driver's license in one go together with confirming the payment, which will create an opportunity for new, simplified user journeys.

EWC | Co-funded by the European Union

This method applies to both browser and app. Some messaging details/steps may vary depending on which one is used.



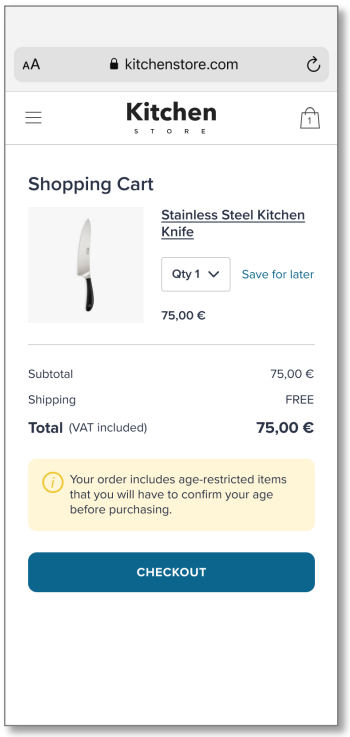
1	Consumer purchases goods and provides payment credentials (or confirms which "stored" credential to use).
2	Merchant requests the Wallet Instance attestation and the Payment Wallet attestation linked to the payment credential. This was placed in the EUDI Wallet at registration. It passes the transaction details and masked card number to the EUDI Wallet. The merchant uses a deep link to invoke the EUDI Wallet on the consumer device or displays a QR code that the consumer can use to invoke the EUDI Wallet.
3	Consumer authenticates to the EUDI Wallet instance.
4	The EUDI Wallet instance asks the user to confirm sharing of the Payment Wallet attestation and Wallet Instance attestation for the purpose of authenticating the transaction with details shown. Consumer confirms sharing for this purpose. The EUDI Wallet provides the authentication data (Payment Wallet attestation, Wallet Instance attestation and cryptographic proof of dynamic linking) back to the merchant.
5	Merchant sends the authentication data in an authentication request to the PSP ACS via the appropriate card network DS. If a token was used the DS calls out the network token platform to detokenize and pass as a PAN to the ACS.
6	ACS approves/declines/challenges authentication request (based on PSP policy). This diagram describes a frictionless approval.
7	PSP ACS sends authentication response back via the appropriate card network DS to Merchant.
8	Merchant confirms authentication success to cardholder.
	Merchant must then proceed to authorisation flow (not covered in this flow).

3.3.2.1 User experience example – mobile browser to app

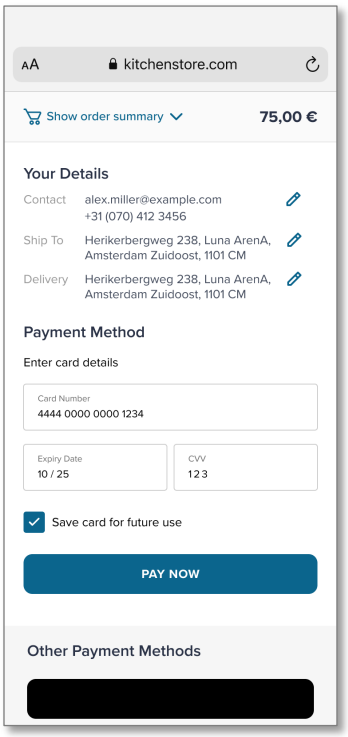
Below an example of the user experience for this flow:

EWC | Co-funded by the European Union

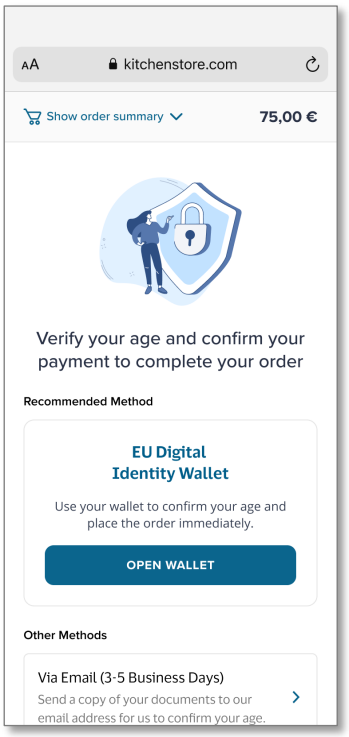
1) User selects (restricted) good at merchant mobile web portal.



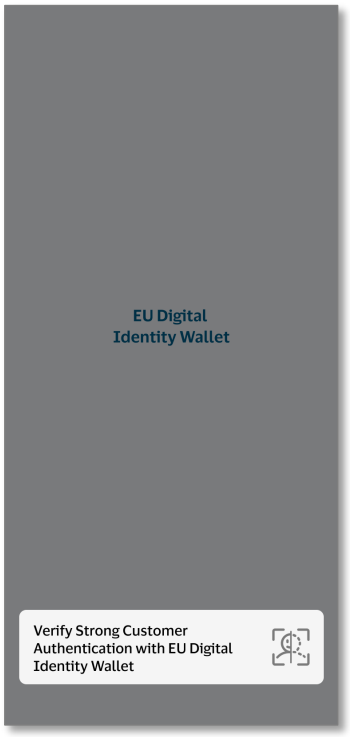
2) User proceeds to checkout.



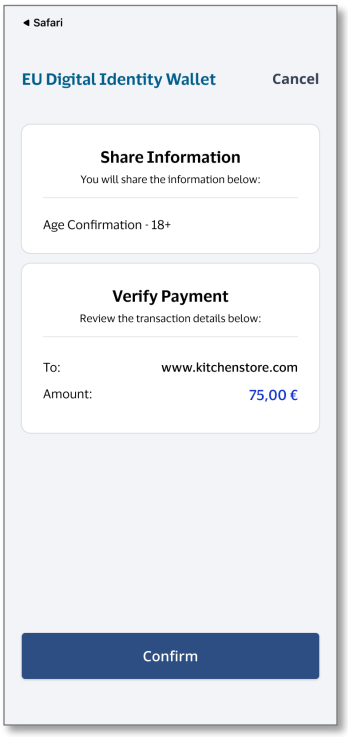
3) User selects EU DI Wallet as means to prove age and confirm payment.



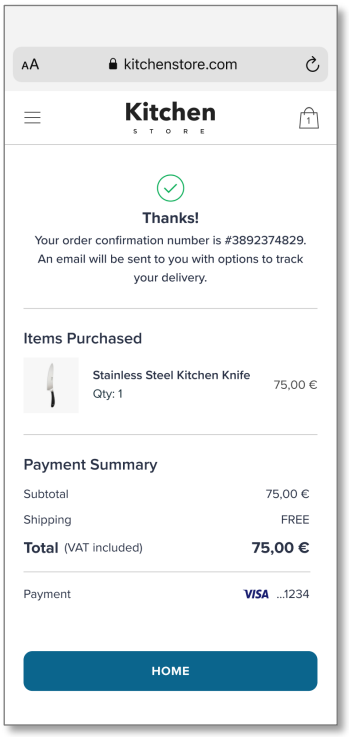
4) User authenticates to EUDI Wallet for the activity of payment confirmation (combined with age verification).



5) EUDI Wallet displays details. User confirms.



6) Merchant displays confirmation.

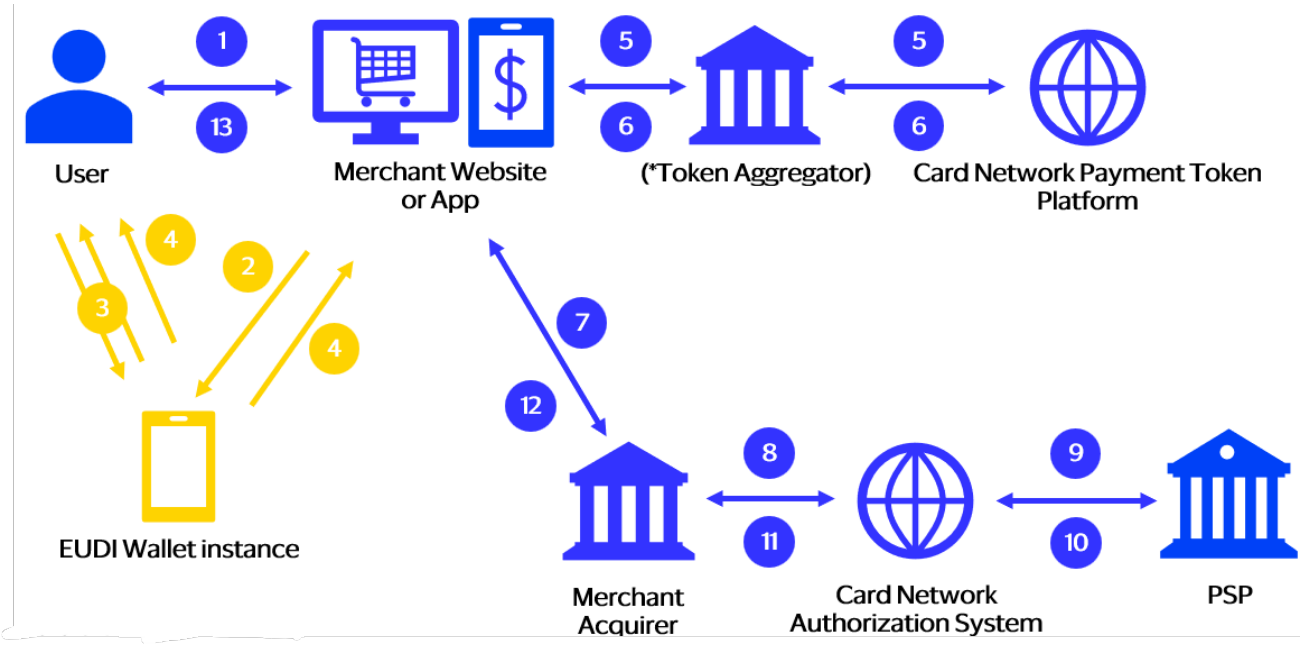


Co-funded by the European Union

3.3.3 Method C: Merchant captured authentication data - with card network payment Token technology

In this method, EMV 3DS is not used to complete the authentication. Instead, the card network provides a payment token platform for use during the authentication process. As such, the exact process may vary slightly from scheme to scheme, but in general, the authentication process is only completed within the card authorisation process itself so the Card Issuer can have the final authentication decision (this explains why the authorisation process is shown in this flow and not in Method A and B where the authentication is fully completed within EMV 3DS).

This method applies to both browser and app. Some messaging details/steps may vary depending on which one is used.



1. Consumer purchases goods and confirms which "stored" credential to use (the merchant held the credential in the form of a payment token).
2. Merchant requests the Wallet Instance attestation and the Payment Wallet attestation linked to the token. This was placed in the EUDI Wallet at registration. It passes the transaction details and masked card number to the EUDI Wallet. The merchant uses a deep link to invoke the EUDI Wallet on the consumer device or displays a QR code that the consumer can use to invoke the EUDI Wallet.
3. EUDI Wallet authenticates cardholder.
4. EUDI Wallet asks the user to confirm sharing of the Payment Wallet attestation and Wallet Instance attestation for the purpose of authenticating the transaction with details shown. Consumer confirms sharing for this purpose. The EUDI Wallet provides the authentication data (Payment Wallet attestation, Wallet Instance attestation and cryptographic proof of dynamic linking) back to the merchant.
5. Merchant sends Authentication data to the appropriate card network token platform - directly or via a Token Aggregator.
6. Card network Payment Token platform validates token (and potentially some authentication data) and returns network cryptogram.
7. to 9. Merchant, via its acquirer, sends authentication data and cryptogram to the Card network authorization system for PSP approval.
10. to 12. PSP approves/declines authentication/authorization and sends response back to merchant via card network and acquirer.
13. Merchant confirms authentication/authorization success to the cardholder.

Consumer returns to Merchant web site or app.

EWC | Co-funded by the European Union

3.4 Responsibilities per actor

3.4.1 EUDI Wallet

For **Method A** the EUDI Wallet must be able to:

- receive a request for a verifiable presentation from the card issuer for the Wallet Instance attestation and the Payment Wallet attestation linked to the PAN. This was placed in the EUDI Wallet at registration. This request may be sent as a push notification, a QR code, or deep link to allow the consumer to switch between merchant site and the EUDI Wallet seamlessly to facilitate SCA,
- as part of this request, it should be able to receive the transaction details from the card issuer and show these to the user (amount, currency and payee/merchant name),
- securely authenticate the user, using the one of the user authentication methods accepted by the card issuer during registration,
- confirm success of authentication to user,
- provide the authentication result (Payment Wallet attestation, cryptographic proof of dynamic linking and Wallet Instance attestation) back to the card issuer's ACS,

Additionally, for **Method B** the EUDI Wallet must be able to:

- receive a request for a verifiable presentation from the merchant for the Wallet Instance attestation and a Payment Wallet attestation. This may be specific to the PAN the user has provided to the merchant at checkout or to the PAN / token that the merchant has on file. This link was established during registration of the EUDI Wallet instance for SCA at the PSP,
- ask the user to select one of the Payment Wallet attestations they added to their EUDI Wallet instance at registration, if the merchant has not requested a Payment Wallet attestation linked to a specific PAN / token
- optionally, receive and process a request for other attestations which the merchant needs for specific use cases (e.g. age restricted goods),
- receive the request may be sent as a QR code for the user to scan, or deep link to allow the consumer to switch between merchant site and the EUDI Wallet seamlessly for SCA,
- receive transaction details from the merchant and show these to the user (amount, currency and payee/merchant name) as part of this request,
- provide the authentication data to the merchant, including cryptographic proof of dynamic linking, the Payment Wallet attestation as proof that the wallet instance can be used to authenticate this transaction.

Method C doesn't have any additional requirements for the EUDI Wallet.

3.4.2 Merchant

For **Method A**, the merchant needs to:

- send an authentication request to the Card Issuer's ACS via the appropriate card network DS.

For **Methods B and C**, the merchant must be able to request authentication data from the EUDI Wallet (Payment Wallet attestation, Wallet Instance attestation and cryptographic proof of dynamic linking). This will be done by the merchant offering the user a list of authentication methods that includes the EUDI Wallet instance held by the user, when the user has registered that EUDI Wallet instance with the PSP for SCA for the account identified by the PAN or token.

Specifically, the merchant must:

- send a verifiable presentation request for the Wallet Instance attestation and a Payment Wallet attestation. This may be specific to the PAN the user has provided to the merchant at checkout or to the PAN / token that

Co-funded by the European Union

the merchant has on file. This link was established during registration of the EUDI Wallet instance for SCA at the PSP,

- the request may be sent as a QR code for the user to scan, or deep link to allow the consumer to switch between merchant site and the EUDI Wallet seamlessly for SCA,
- send the transaction details (amount, currency and payee/merchant name), as part of this request, so that the EUDI Wallet instance can display them to the user.
- potentially receive the card credentials i.e. token, where the merchant did not request a specific Payment Wallet attestation and the user made a choice of card, by select a specifying a Payment Wallet attestation in their EUDI Wallet instance.
- send the authentication data (Payment Wallet attestation, Wallet Instance attestation and cryptographic proof of dynamic linking) together with the credential details (in the form of a PAN or payment token) to the card network Directory Server (Method B) or TSP (Method C) as part of the authentication request.

3.4.3 PSP

For **Methods A, B and C** the Card Issuer should validate:

- the Payment Wallet attestation received was issued by them and is linked to the PAN / token in the authentication request. This link was established during registration of the EUDI Wallet instance for SCA at the PSP,
- that the cryptographic proof of dynamic linking received was signed using the key bound to the Payment Wallet attestation received and relates to the transaction details the PSP has received in the authentication request,
- the Wallet Instance attestation received indicates that the wallet is still in a “valid” state and that the wallet provider is still on the Trusted List.

EWC | Co-funded by the European Union

4.SCA for account-based transactions

This section covers using the EUDI Wallet for SCA during account-based transactions. Instead of a card number the customer uses a **payment account (IBAN, International Bank Account Number)** for payment. This is often referred to as 'pay-by-bank'.

4.1 Pre-conditions

The following pre-conditions apply:

1. Before the EUDI Wallet can be used to authenticate a payment transaction, it must be registered for strong authentication (SCA) with the user's Payment Service Provider (PSP). This process is described in section 2 of this document.
2. The merchant is working with a PISP that connects to the payer's ASPSP. The payer will need to identify the ASPSP from where they want to make the credit transfer in the check-out flow offered by the PISP via the merchant.
3. To activate the EUDI Wallet, the payer is not required to provide the customer-ID or the source account details. The ASPSP can retrieve this information directly from the EUDI wallet when starting the authentication flow. The payer will only be able to select the source accounts for the payment that have been registered in the EUDIW.

If any of these pre-conditions are not met, the EUDI wallet cannot be used as the authentication mechanism for the account-based transaction.

4.2 Actors

- User / Payer
- Merchant
- Payment Initiation Service Provider
- PSP (role: Relying Party)
- EUDI Wallet or basic EUDI Wallet
- Trusted List Provider

4.3 High-level SCA Account Flows

Every PSP has a different API for account-based transactions, and therefore there may be differences in flow. While not all PSPs allow the payer to change (or select) the payment account during the authentication flow, since the EUDI wallet will hold one or more IBANs, the user must be able to select or change the default source account from where the payment is credited.

There are potentially two methods:

- Method A: SCA during Payment Initiation, and
- Method B: SCA using a signed payment request.

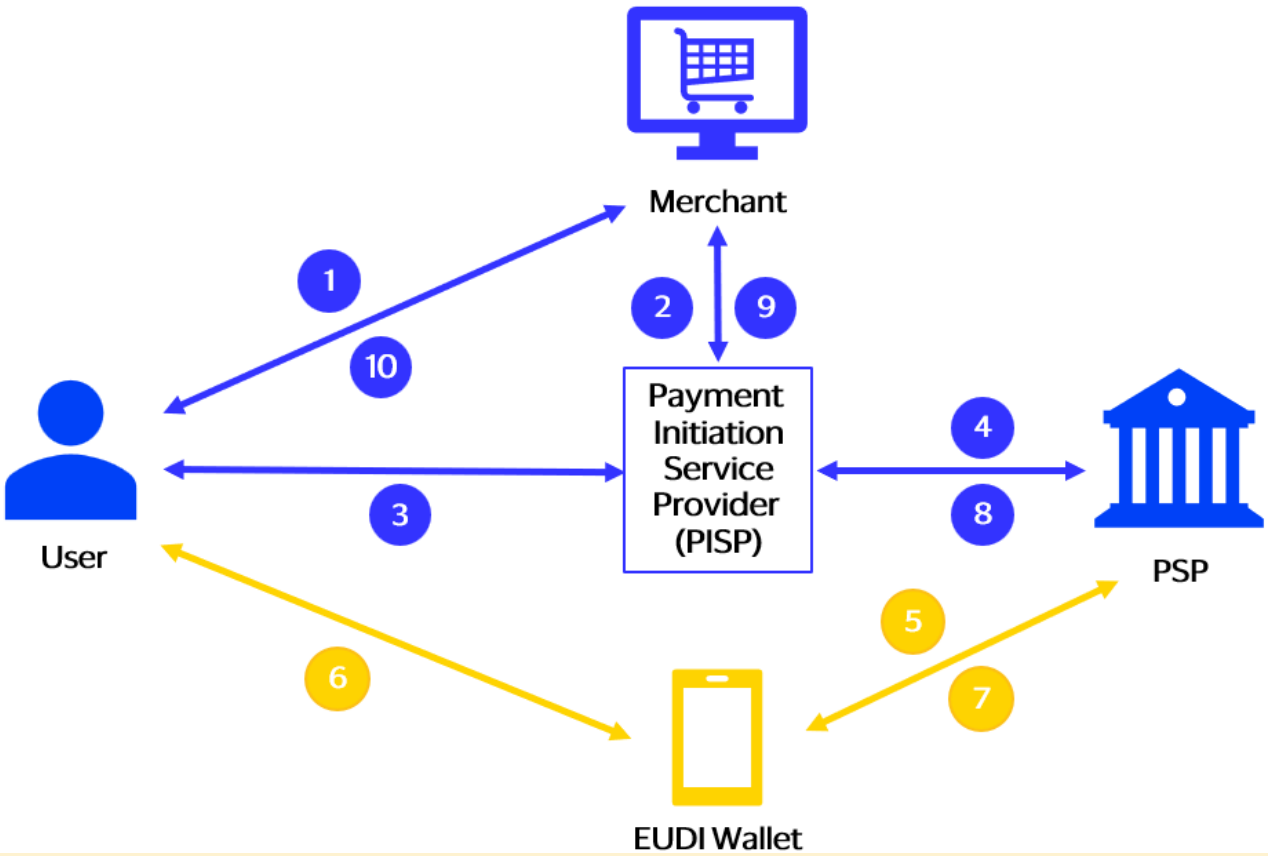
This document only covers Method A. Method B is still subject to discussion and will not be presented here.

4.3.1 Method A: SCA Account during Payment Initiation

This first Method A describes a 'standard SCA journey' where — after obtaining consent from the payer — the PISP uses an API to submit a payment order to the ASPSP. This payment order payee details (e.g. name and IBAN of the

EWC | Co-funded by the European Union

destination account), along with a preference for the SCA to be completed using one of the registered EUDI Wallet – if available.



1. User requests check out from merchant.
2. Merchant provides payment information to PISP.
3. PISP summarises payment and requests explicit consent for initiation.
4. PISP sends payment order to PSP for initiation.
5. PSP enforces SCA by activating the EUDI Wallet.
6. EUDI Wallet instance displays transaction details and authenticates payer.
7. EUDI Wallet sends authentication result to PSP. This includes the Payment Wallet attestation placed in the EUDI Wallet at registration.
8. PSP informs the PISP of payment initiation success or failure.
9. PISP informs merchant of payment status.
10. Merchant confirms payment and releases goods or service.

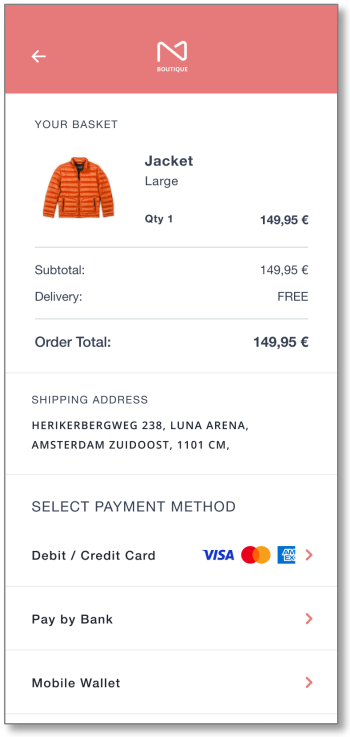
4.3.1.1 User experience example – app to app

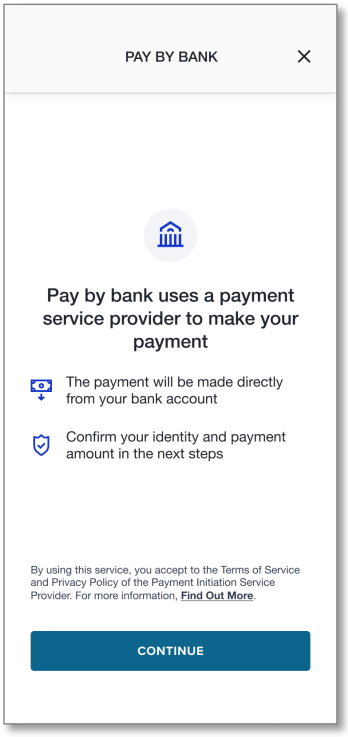
Below an example of the user experience for this flow:

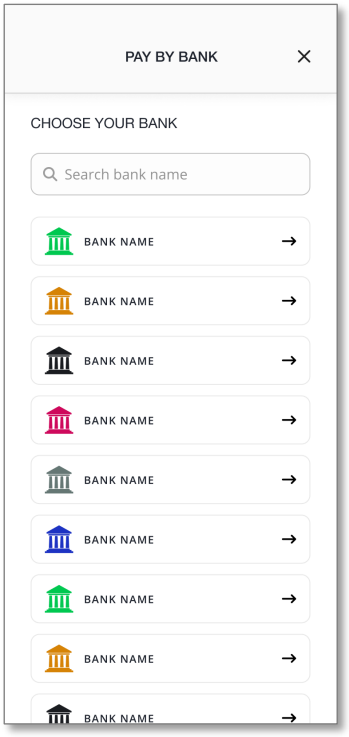
1) User makes purchase on merchant app and selects 'Pay by bank'.

2) User consents to using the PISP.

3) User selects their bank.



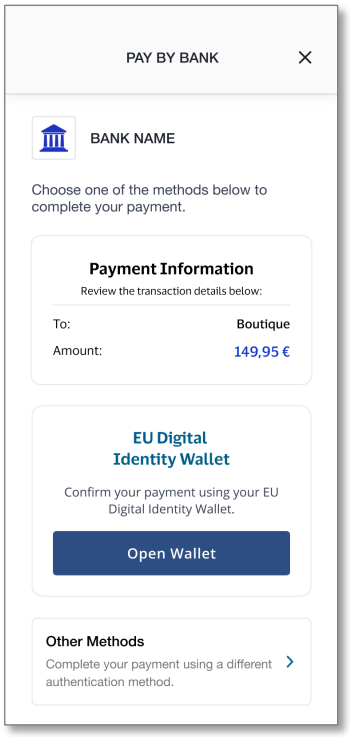


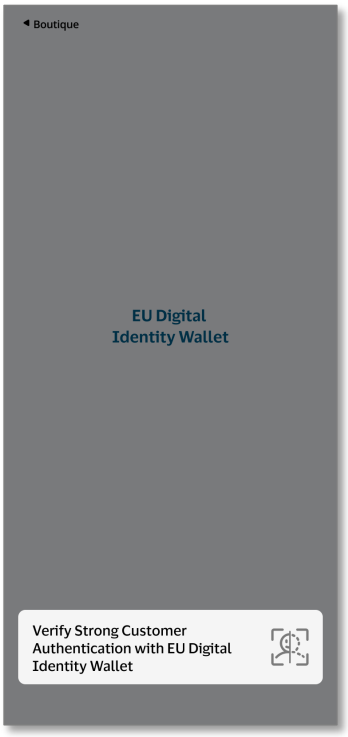


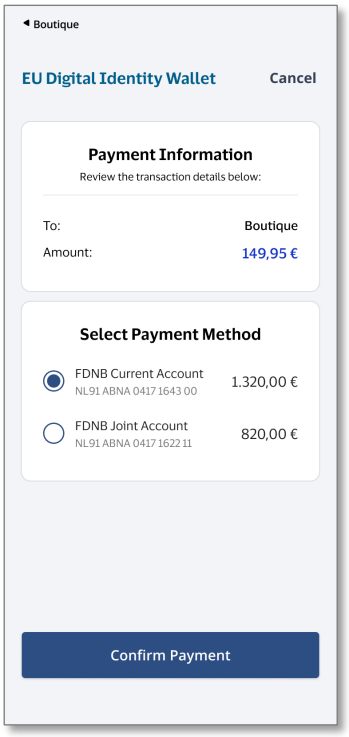
4) Merchant app displays button to open EUDI Wallet. User taps.

5) User authenticates to EUDI Wallet for the activity of payment confirmation.

6) User selects account from which to make payment. User confirms.

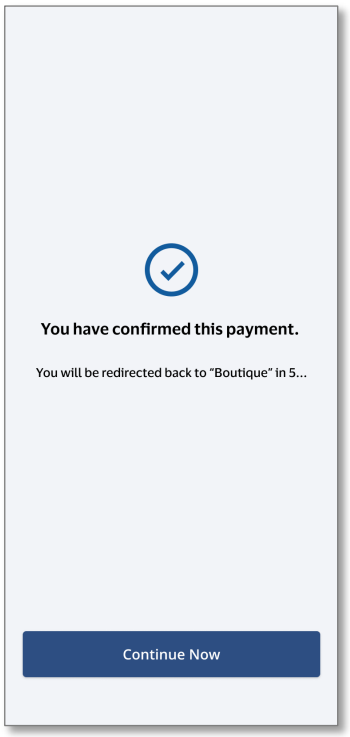




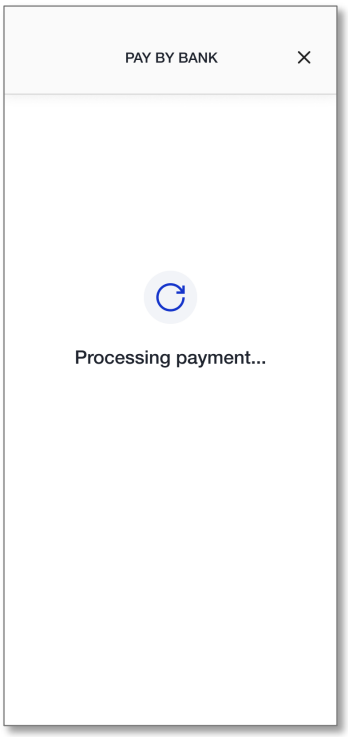


Co-funded by the European Union

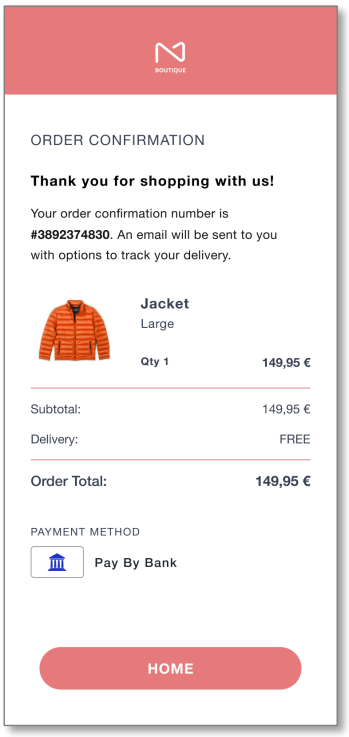
7) User is displayed confirmation and automatically redirected to merchant.



8) PISP displays a processing animation while confirming payment status and successful initiation.



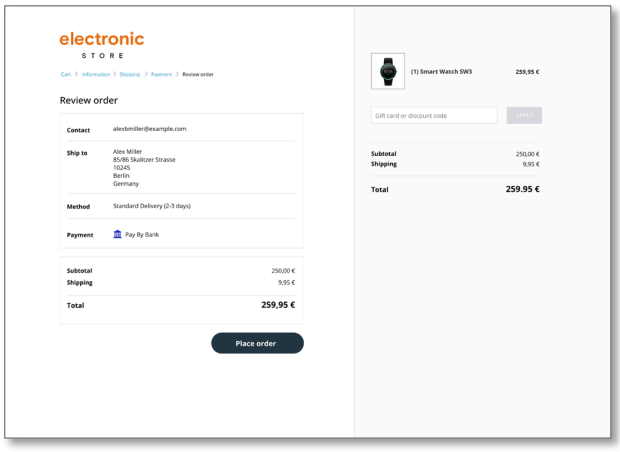
9) Merchant app displays confirmation message.



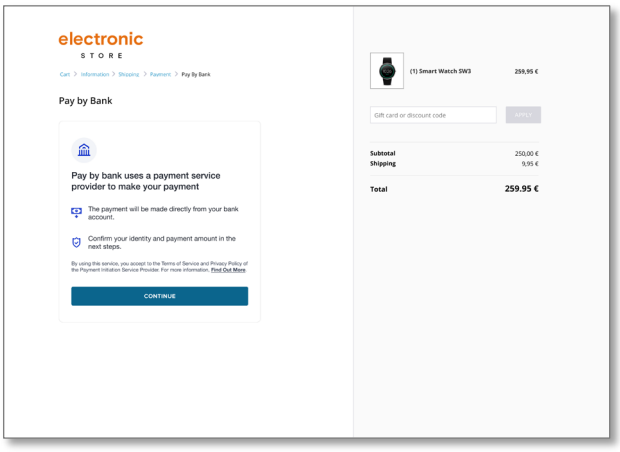
4.3.1.2 User experience example – desktop to app

Below an example of the user experience for this flow:

1) User makes purchase on merchant ecom site and selects Pay by bank.

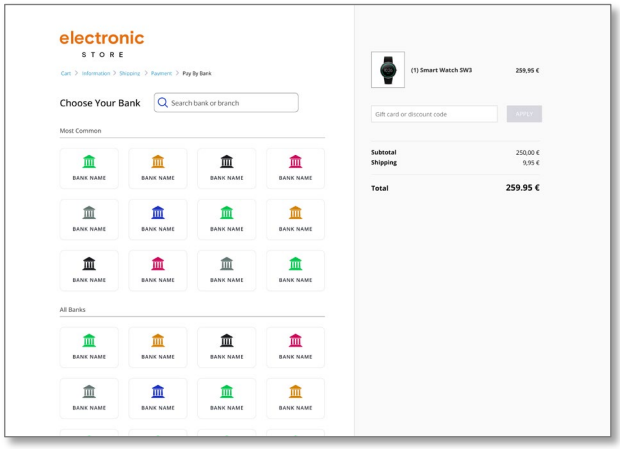


2) User consents to use pay by bank.

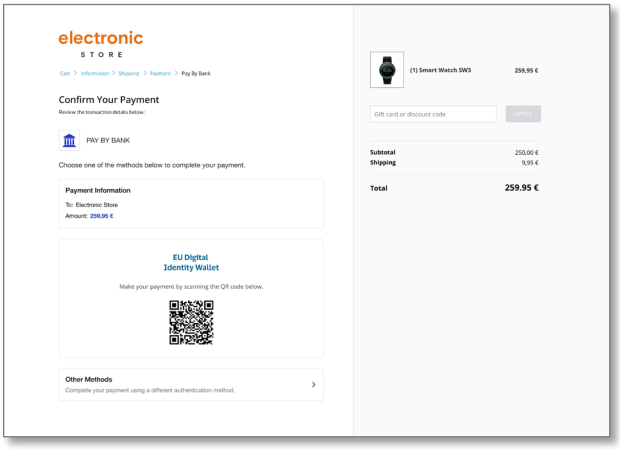


EWC | Co-funded by the European Union

3) User selects their bank.

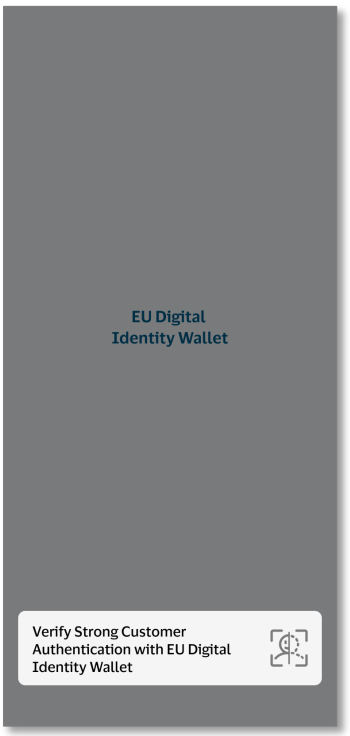


4) Merchant site displays QR code for user to scan with EUDI Wallet.



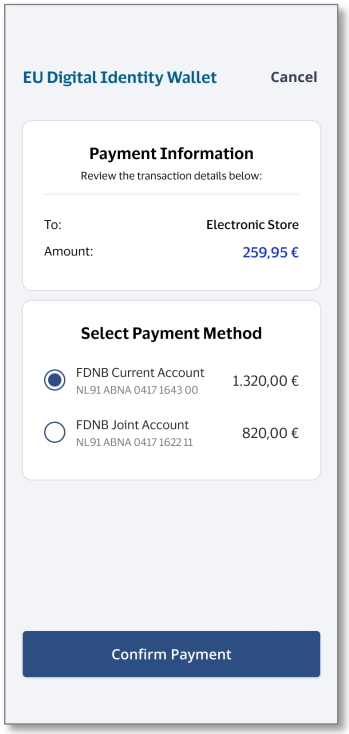
5) User scans QR code with EUDI Wallet.

6) User authenticates to EUDI Wallet for the activity of payment confirmation.

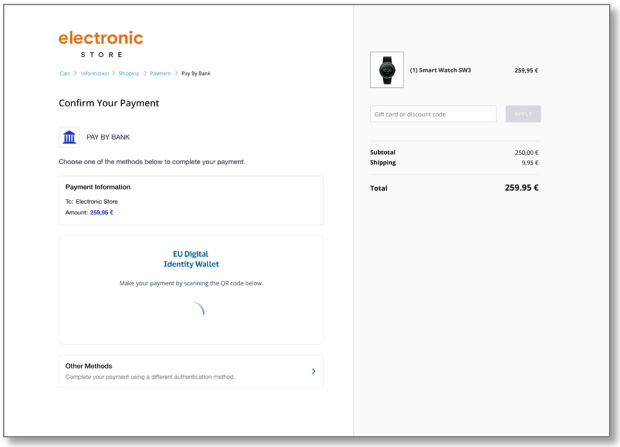


Co-funded by the European Union

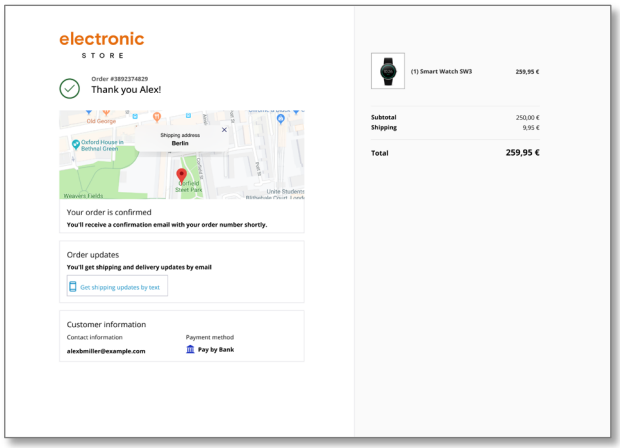
7) User selects account from which to make payment. User confirms.



8) Merchant processes payment, while the PISP is confirming payment status and successful initiation.



9) Merchant ecom site displays confirmation.



EWC | Co-funded by the European Union

4.4 Responsibilities per actor

4.4.1 EUDI Wallet

For **Method A** the EUDI Wallet must be able to:

- Automatically activate ("launch") on the device of the payer for the authentication.
- Receive a request for a verifiable presentation from the PSP for the Wallet Instance attestation and the Payment Wallet attestation linked to the payment account, if supplied; or if not supplied, a Payment Wallet attestation chosen by the user for a payment account they hold. This was placed in the EUDI Wallet at registration with their PSP. The selection of the attestations by the user resembles the selection of the source of funds for the payment. The request for the verifiable presentation may be sent as a QR code, or deep link to allow the consumer to switch between merchant site / app and the EUDI Wallet seamlessly to facilitate SCA.
- As part of this request, the EUDI wallet should be able to receive the transaction details from the PSP and inform the payer that the authentication request for a specific payment (currency, amount and merchant name) is pending.
- Securely authenticate the user, using the one of the user authentication methods accepted by the PSP during registration.
- Confirm success of authentication to user.
- Provide the authentication result (Payment Wallet attestation, cryptographic proof of dynamic linking and Wallet Instance attestation) back to the PSP.
- In the case of an app-to-app redirection, the EUDI Wallet must automatically redirect the payer back to the PISP or merchant environment.

4.4.2 Merchant

For **Method A**, the merchant must be able to:

- send the payment information to the PISP. This information must include the amount to be paid, payment reference, merchant's name, merchant`s recipient account number (i.e., IBAN), and the account holder name of the recipient account; and
- If available on file, provide the payer's IBAN.

4.4.3 PISP

For **Method A** the PISPs responsibilities are:

- Obtain consent to initiate a payment for the payer.
- To identify the payers's PSP
    - if available, request the payer's IBAN from the merchant to infer the PSP; or
    - Ask the payer to identify the PSP from where they wish to initiate the payment.
- Summarise the payment details for the payer to confirm.
- Connect to an access interface[4] provided by the PSP that supports the EUDI Wallet for SCA;
- Request the PSP to authenticate the payer using a registered EUDI Wallet, if possible.;
- Submit the payment order to the PSP through the access interface.

[4] An access interface as defined by Commission Delegated Regulation (EU) 2018/389 (i.e. RTS for SCA CSC) Article 30, typically in the form of a dedicated interface or "PSD2 API".

Co-funded by the European Union

- Receive from the access interface the final payment status.
- Inform the merchant about the success or failure of the payment.

4.4.4 PSP

For **Method A**, the PSP must be able to:

- Receive the payment order from the PISP through the provided access interface,
- Provide the EUDI Wallet with:
    - the transaction details (currency, amount and payee name);
    - display the amount and payee name, as per the dynamic linking requirements in PSD2;
    - and, optionally, a unique identifier (typically in the form of an IBAN), if provided by the PISP
- Support app-to-app redirection for the registered EUDI Wallet,
- Display a landing page that offers the payer to start the EUDI Wallet instance if the user is on a different device.
- Return the status of the payment to the PISP.
- The PSP should validate:
    - the Payment Wallet attestation that was issued and is linked to the IBAN in the authentication request. This link was established during registration of the EUDI Wallet instance for SCA at the PSP,
    - the cryptographic proof of dynamic linking received that was signed using the key bound to the Payment Wallet attestation received and relates to the transaction details transmitted by the PISP,
    - the Wallet Instance attestation received indicates that the wallet is still in a “valid” state and that the wallet provider is still on the Trusted List.

EWC | Co-funded by the European Union

A Appendix

A.1 EWC Payment Taskforce

Starting with a strong belief that Payment is a key use case to drive usage and therefore adoption of EUDI Wallets, EWC has formed in 2023 its Payment Taskforce, led by Visa, with the objective of

- defining the EUDI Wallet payment specifications, build and pilot selected payment use cases
- identify barriers to adoption and evaluate opportunities in payment beyond SCA, in particular by provisioning a card or account token in the EUDI Wallet and initiate an online or in-store payment
- use those specifications and findings to give feedback and offer inputs to the European Commission and future Payment and/or Digital Identity standards

Our guiding principles have been:

- include both card and account payments
- minimize the impact on existing payment infrastructure
- innovation by bringing together payment and identity credential (e.g age verification in one SCA)

List of EWC Payment Taskforce active members (as of 21st October 2024)

Wallet providers:

- BankID (Sweden)
- Digidentity (Germany)
- iGrant (Sweden)
- Infocert (Italy)
- Lissi (Germany)
- University of the Aegean (Greece)

Banks

- Banca Transilvania (Romania)
- Piraeus Bank (Greece)
- Raiffeisen Bank (Austria)

Payment experts

- Netcetera (Switzerland)
- Outpayce by Amadeus (UK)
- Tink (Sweden)
- Token ID (Netherlands)
- Visa (UK)
- Worldline (France)

Co-funded by the European Union