P

Payment Initiation using EUDI Wallets – Implementation Guide

PROVISIONING OF PAYMENT CREDENTIALS TO AND PAYING WITH THE EUROPEAN UNION DIGITAL IDENTITY WALLET (EUDIW)

Document properties

Name	Payment Initiation using EUDI Wallets
Document Version	1.0
Status	Approved
Publication date	October 21, 2024
Contact	EURotterdamTrainingAndDoc@visa.com
Authors	Rahmat Adnan, Marie Austenaa, Laurent Bailly, Stan van Haasteren, Stefan Kauhaus, Ranjiva Prasad, Xiaoman Xu

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	2nd of April 2024	• Created first draft	Draft
0.2	5th of April 2024	• Fixed errors and added section on redirection methodology	Draft
0.3	22nd of May 2024	• Adding content about authenticated SCA card payments	Draft
0.3.1	30th of May 2024	• Implementing edits from workshop, changing acquirer to payee PSP	Draft
0.3.2	5th of July 2024	• Changed template	Draft
0.4	20th of September 2024	• Sharpened focus on card transactions and device tokens; updated images in new style	Draft
1.0	17th of October 2024	• Version after final review • Updated UX samples • Added CC licence and authors • Added Payment taskforce appendix	Approved

EWC | Co-funded by the European Union

Table of contents

Co-funded by the European Union

1.Overview

In the evolving digital economy, users increasingly want to use their mobile device to pay both in-store and online. This process must be secure:

- It must not unduly expose credentials, and
- the user must be strongly authenticated (unless an exemption applies).

This Implementation Guide describes the provisioning of payment credentials to the EUDI Wallet (European Union Digital Identity Wallet). It also covers paying with these payment credentials stored in the EUDI Wallet. Payment credentials can represent both cards and accounts. This document outlines the usage scenario, process flow, and technical requirements for using the EUDI Wallet to request and capture card credentials for payments. The goal is to provide a secure, efficient, and user-friendly solution for payment transactions that meets regulatory requirements and delivers an enhanced shopping experience for users.

The EU regulation on electronic identification and trust services aims to 'support the adoption and use of the EUDI Wallet by integrating them with the ecosystem of public and private digital services.' Mobile payment wallets are an important private digital service that European consumers increasingly use, but current solutions tend to be domestic and lack interoperability.

EUDI Wallets are a logical match for payments as they are required to provide authentication functionality, which is a key part of payments. Adding the support for payment authentication to EUDI Wallets is an opportunity to expand the functionality of the EUDI Wallet with a real potential to scale.

Payment credentials representing a 'funding source' must first be provisioned securely to an EUDI Wallet for it to be used as a payment instrument. The funding source in the context of this document is a payment card, represented by a card number or Primary Account Number (PAN), typically 16 digits written on the payment card.

Payment tokens

The payment credentials must be stored securely to meet the Payment Card Industry Data Security Standard (PCI DSS) requirements. It is best practice to store **Payment Tokens** in the authentication device, rather than the real payment credentials. A Payment Token is a unique identifier generated by a Token Service Provider (TSP) as an alternative for a PAN and is usable only in a specific context. The TSP in the context of this document is a service provided by the payment network (Visa, Master Card, American Express etc).

Using a Payment Token instead of a PAN enhances security as it cannot be reversed to reveal the original payment credentials, so the actual credentials are never exposed to merchants before payment execution and in case of leak/theft the exposed tokens are of little use to malicious entities. Therefore, tokenisation mitigates fraud.

EWC | Co-funded by the European Union

On average, token-based transactions have a higher approval rate compared to traditional electronic payments. As a result, tokenisation improves payment experiences and increases merchant revenue.
Within the scope of this document, the EUDI Wallet is device-based; meaning a user is required to install an EUDI Wallet on their device (mobile or tablet). A **device token** obtained from a network TSP will be generated and provisioned to the EUDI Wallet installed on the device. Usually, the EUDI Wallet provider's server component connects to the TSP via a Token Requestor Aggregator (TRA). Once the token has been provisioned, it can only be used for payments with the EUDI Wallet instance on this device. If the user wants to use the same credentials on a different device, provisioning needs to start from scratch.

SCA

European regulations require Strong Customer Authentication (**SCA**), which must be completed both:

- when provisioning the payment credential to a payment wallet, and
- when a payment is made.

This authentication process can create friction and negatively impact payment completion. Therefore, it is essential that both authentication processes perform smoothly to maximise the likelihood of completion of both provisioning and payments.
SCA requires that the payer is authenticated through at least two factors, which must be independent from the other and from two of the three categories listed below:

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

Using EUDI Wallets as a mobile payment wallet addresses these topics by providing a secure platform for storing tokenised payment credentials and enabling a state-of-the-art authentication experience based on the regulatory requirements towards identity wallets.

1.1 Audience

This document is aimed at:

- ARF experts drafting detailed specifications to enable the EUDI Wallet for provisioning and payments,
- EUDI Wallet providers who need to know how to enable provisioning of cards and using them in a payment transaction,
- Payer's PSP (e.g. Banks) and their authentication services providers (such as ACSs) who must ensure their cards can be provisioned to an EUDI Wallet and used in transactions,

EWC
Co-funded by the European Union

- Payee (e.g. Merchant) and payee PSP (e.g. Acquirer) who are looking for implementing new capabilities of the EUDI Wallet for card payment transactions.

1.2 Terms and Actors

Architecture and Reference Framework (ARF): Provides the specifications needed to develop an interoperable EUDI Wallet Solution based on common standards and practices.
Attestation: A signed set of attributes, see Electronic Attestation of Attributes (EAAs)
Payment Wallet Attestation: Attestation issued to an EUDI Wallet instance by an EAA provider 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) – entity who issued 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. Example 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.
Device-based wallet: A wallet that can only be accessed by the user from the device on which it is installed.
Electronic Attestation of Attributes (EAAs): An attestation in electronic form that allows the authentication of attributes – eIDAS Regulation proposal.
European Union Digital Identity Wallet (EUDI Wallet**):** The EUDI Wallet instance used for SCA and storing payment credentials to be used for financial transactions.
European Union Digital Identity Wallet (EUDI Wallet**) provider:** Provider of EUDI Wallet instances to users. The provider has a back-end component which connects to wallet instances and other parties.
Holder: An entity that receives Verifiable Credentials 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.
Issuer: A provider issuing Person Identification Data (PID) or (Q)EAAs. In the case of the EUDI Wallet there may be multiple Issuers for PID and (Q)EAA.

EWC | Co-funded by the European Union

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. The Merchant is the one initiating a user's authentication request during a payment transaction.
Payer/PSU (payment service user)/User: Holder of a EUDI Wallet and of a card 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 enabled EUDI Wallet: a wallet that stores payment credentials to be used during a financial transaction.
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 A Card-Based Payment Instrument Issuer.
Relying Party (RP): The party that receives information from the wallet.
Token Requestor (TR): A provider registers with one or more TSPs to request Payment Tokens. An EUDIW provider can act as token requestor.
Token Requestor Aggregator (TRA): A provider of payment token services to a merchant or EUDI Wallet 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 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.

1.3 Use cases

This document describes the following use cases:

- Provisioning of tokenised card credentials (Section 2)
- Paying with tokenised card credentials (Section 3)

Please note: the use case described in Section 2 is a precondition for the use case described in Section 3.

EWC | Co-funded by the European Union

2.Provisioning of tokenised card credentials

This section describes how to tokenise and securely store card credentials in the EUDI Wallet so they can later be used for payments.

A device token is requested from a network TSP, usually via a TRA. The TRA determines based on the first digits of the card number to which network TSP (Visa, Master Card etc) the request must be routed. Once the token is returned, it is provisioned to the EUDI Wallet. When performing SCA for a payment with such a device-based token, this can also ensure the 'possession factor', because the user owns the device. Two methods for token provisioning have been defined:

- Method A.1: Provisioning from PSP app EUDI Wallet instance
- Method A.2: Provisioning from EUDI Wallet instance

2.1 Pre-conditions

Before the provisioning process can start, the following must be true:

1. The EUDI Wallet provider must be able to support additional configurations, including EMV Contactless Specifications for payment systems, ISO/IEC 7816 and ISO/IEC 14443.
2. The user must have an EUDI Wallet instance from a "valid" wallet solution, from an EUDI Wallet provider, present on the Trusted List Providers (TLPs) and the EUDI Wallet instance must have a "valid" status.
3. The EUDI Wallet provider must be onboarded to the Token Service Provider (TSP) as a Token Requestor (TR) before the EUDI Wallet can request a token from the TSP.

   3.1. Once the EUDI Wallet provider is onboarded to the Token Service Provider (TSP), it will receive its Token Requestor ID from the TSP. The TRID is used by the TSP to identify the Token Requestor (TR). If the EUDI Wallet provider connects with the TSP directly, it will perform a keys and certificates exchange with the TSP through the TSP's web service API.

   3.2. The EUDI Wallet provider must be onboarded to the Token Requestor Aggregator (TRA) if it connects with the TSP via a TRA. The EUDI Wallet provider will perform a keys and certificates exchange with the TRA through the TRA's web service API.

An additional precondition applies to Method A.1:

4. The EUDI Wallet provider must have implemented the 'push provisioning' service specified by the Token Service Provider and the card issuer.

2.2 Actors

The following actors play a role in this use case:

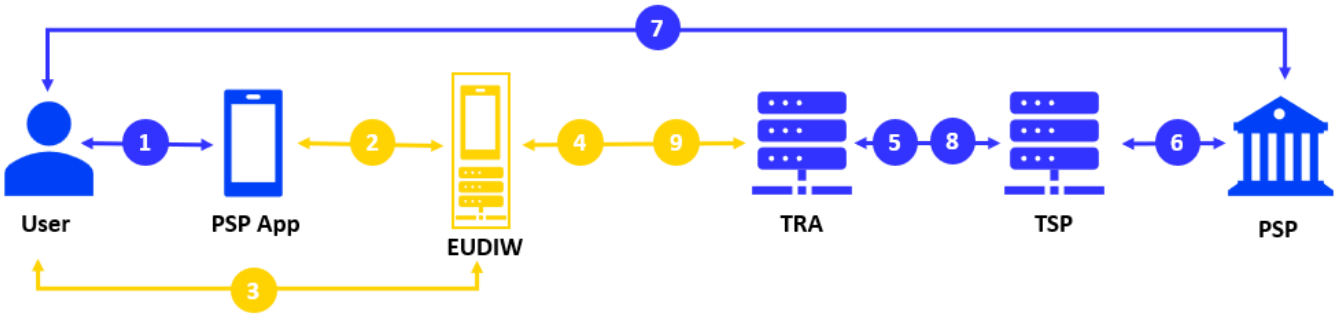
EWC | Co-funded by the European Union

- User
- PSP (card issuer)
- EUDI Wallet Instance
- EUDI Wallet Provider
- Token Service Provider
- Token Requestor
- Token Requestor Aggregator

2.3 High-level Provisioning flows

2.3.1 Flow Method A.1: Provisioning from PSP app to EUDI Wallet

In Method A.1, the user starts with their PSP app, which will 'push' the card data to the EUDI Wallet. It is therefore sometimes referred to as 'push provisioning'.



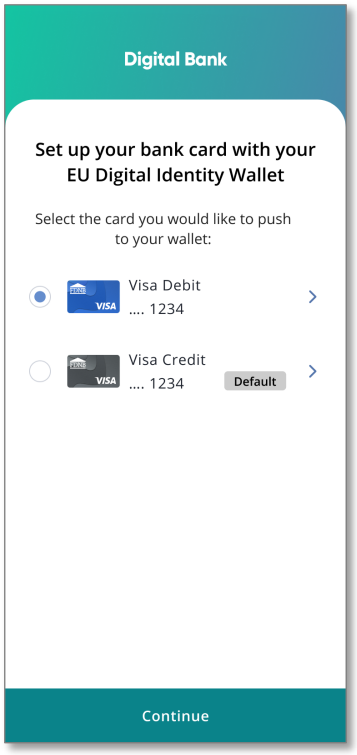
1. User logs into PSP app and navigates to the "share your cards with other trusted parties" feature. User selects a card to be shared, and the PSP app presents a list of participating digital wallets from which the user may select. User selects the EUDI Wallet provider of their EUDI Wallet instance.
2. The PSP app launches the EUDI Wallet instance and shares the corresponding push data with it based on the TSP push provisioning specifications.
3. User logs into EUDI Wallet and consents to adding the pushed card to the EUDI Wallet.
4. EUDI Wallet provider initiates the tokenise request to the TRA with the push data received from the PSP.
5. The TRA passes the tokenise request to the relevant TSP.
6. TSP sends tokenise request to PSP for approval. PSP responds with approval and indicates whether SCA is required to activate the token.
7. Optional: User performs SCA if it is required by the PSP. Several options are available for this. One particularly noteworthy option is for the user to present the Payment Wallet Attestation to the PSP as described in the SCA Implementation Guide.
8. The TSP returns a token to the TRA.

EWC | Co-funded by the European Union

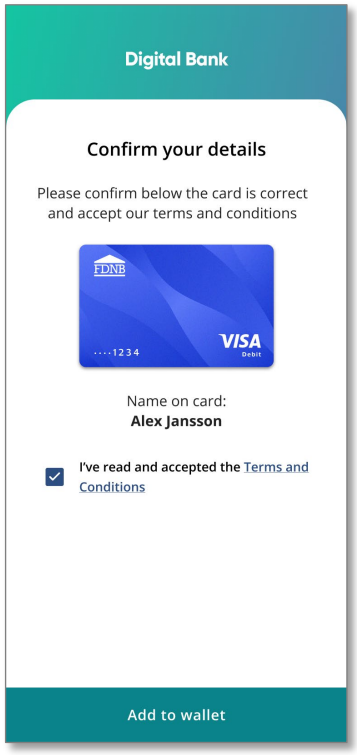
9. The device token is provisioned to the EUDI Wallet instance, and an ‘Add Card successful’ message is displayed to the user. The user can now use the tokenised card provisioned to the EUDI Wallet for payments.

2.3.1.1 User experience example – app to app

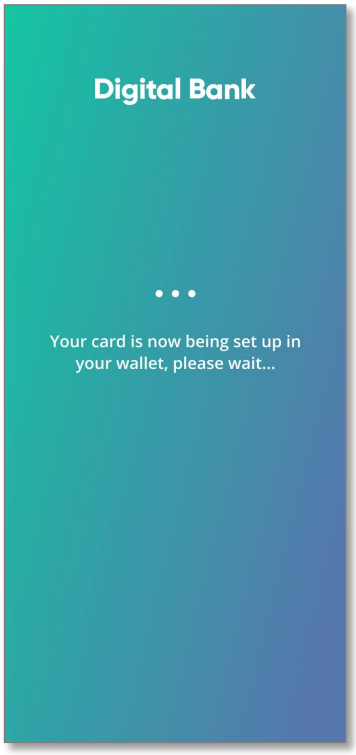
Below an example of the user experience for this flow:



In PSP app, user selects card to be added to EUDI Wallet.

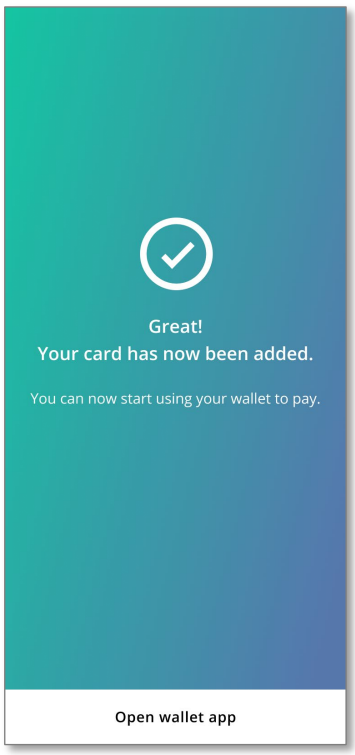


User accepts terms and conditions and continues.

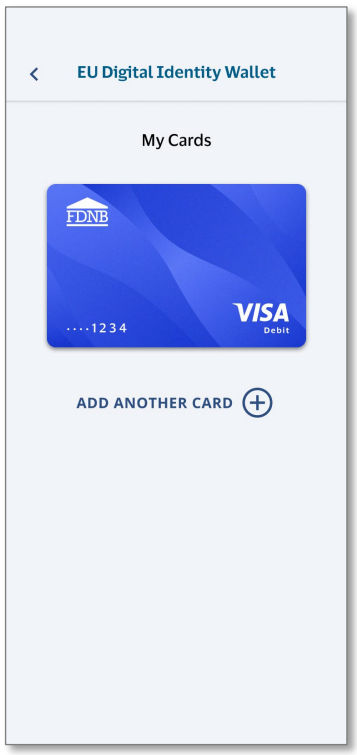


PSP shares card data with EUDI Wallet.

EWC
Co-funded by the European Union



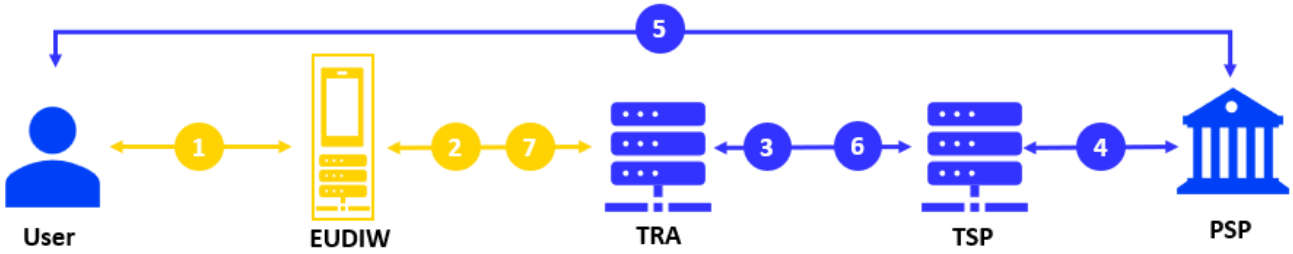
PSP app displays confirmation that card has been added to EUDI Wallet.



EUDI Wallet is launched, and card is displayed.

2.3.2 Flow Method A.2: Provisioning from EUDI Wallet instance

Method A.2 is triggered by the user starting card provisioning by selecting an option available in the EUDI Wallet menu. In this method, the user is not logged into the PSP app. Therefore, the PSP requires additional verification to confirm the user's identity prior to the tokenisation process.



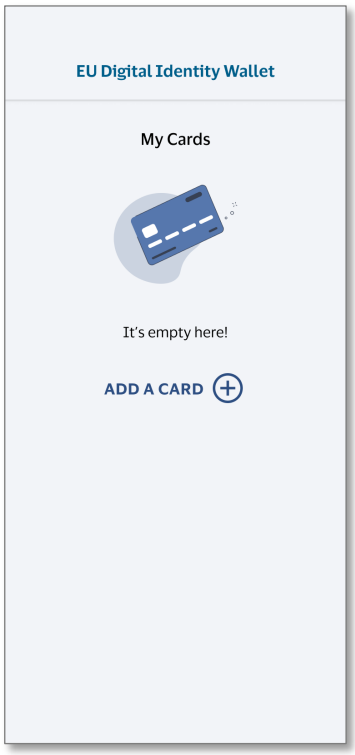
1. User logs into the EUDI Wallet instance and selects to add a payment card to the EUDI Wallet. The card number can be provided by manually entering it into the EUDI Wallet or using other secure methods, in compliance with the payment networks' rules and guidelines, such as the Tap to Add Card feature.
2. EUDI Wallet provider sends the tokenise request to the TRA with the card credentials received from the user.
3. The TRA passes the tokenise request to the relevant TSP.

EWC | Co-funded by the European Union

4. TSP sends tokenise request to PSP for approval. PSP responds with approval and indicates that SCA is required to activate the token.
5. User performs SCA against the PSP. Several options are available for this. One particularly noteworthy option is for the user to present the Payment Wallet Attestation to the PSP as described in the SCA Implementation Guide.
6. The TSP returns a token to the TRA.
7. The device token is provisioned to the EUDI Wallet instance, and an 'Add Card successful' message is displayed to the user. The user can now use the tokenised card provisioned to the EUDI Wallet for payments.

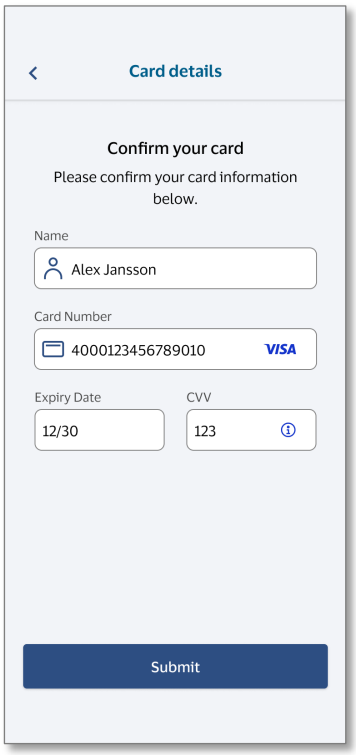
2.3.2.1 User experience example – app to app

Below an example of the user experience for this flow:



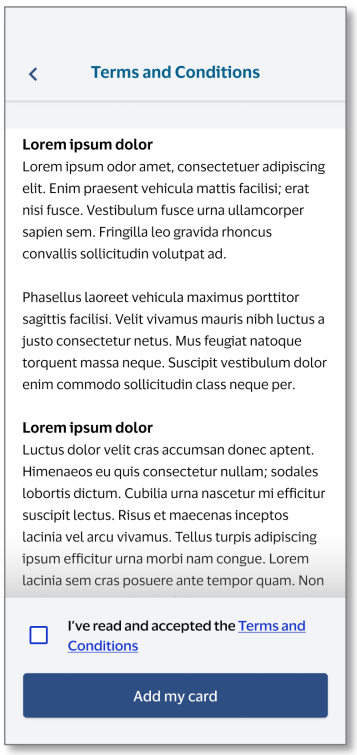
User is logged into EUDI Wallet and decides to add a card.

User scans card or opts to enter details manually.

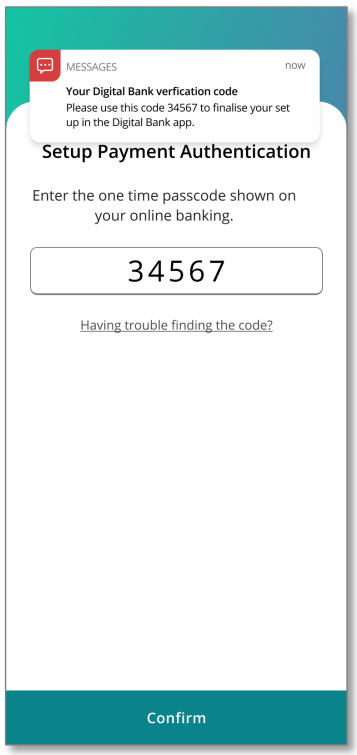


Card details are displayed. User confirms.

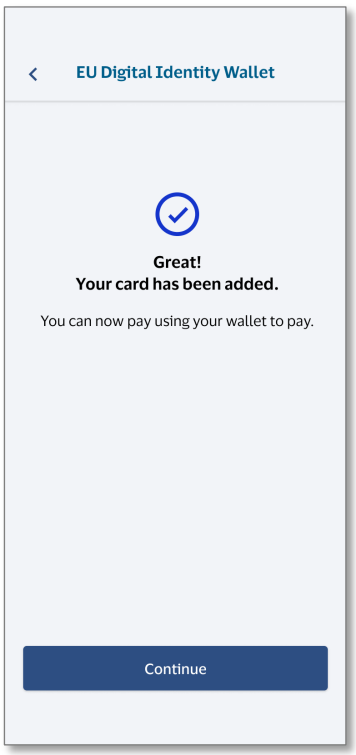
EWC | Co-funded by the European Union



Terms and conditions are displayed. User accepts and taps Add my card.



User is being redirected to PSP for authentication. (OTP method is illustrative.)



A message is displayed confirming that card has been provisioned successfully.

Card is displayed in wallet.

EWC
Co-funded by the European Union

3.Paying with tokenised card credentials

This section describes how to use a tokenised payment card stored on a EUDI Wallet to make payments. These payments can be in-store or online. The aim is that the EUDI Wallet contributes to a secure and user-friendly shopping experience by handling the authentication seamlessly like existing mobile payment wallets that meet regulatory requirements. The payment token, stored securely in the EUDI Wallet, can act as a possession factor in the payment process, because it is bound to a device owned by the user. Protection of the EU DI wallet instance, e.g. via password or biometrics, can serve as second authentication factor.

During the transaction, the EUDI Wallet calculates a cryptogram in which the transaction amount, payee details, and a random number are input parameters. Therefore, the cryptogram is unique for each transaction.

Two methods for payment have been defined:

- Method A.1: Authenticated in-store payment with device-based EUDI Wallet,
- Method A.2: Authenticated online payment with device-based EUDI Wallet.

3.1 Preconditions

Before using the EUDI Wallet to pay with tokenised card credentials, the following must be true:

1. The EUDI Wallet provider must be able to support additional configurations, including EMV Contactless Specifications for payment systems, ISO/IEC 7816 and ISO/IEC 14443.
2. The user must have an EUDI Wallet instance from a “valid” wallet solution, from an EUDI Wallet provider that is present on the Trusted List Providers (TLPs)
3. The EUDI Wallet instance must have a “valid” status.
4. The user must have completed provisioning of a tokenised payment card on an EUDI Wallet which can act as a possession authentication factor for the payments (see section 2).

3.2 Actors

The following actors play a role in this use case:

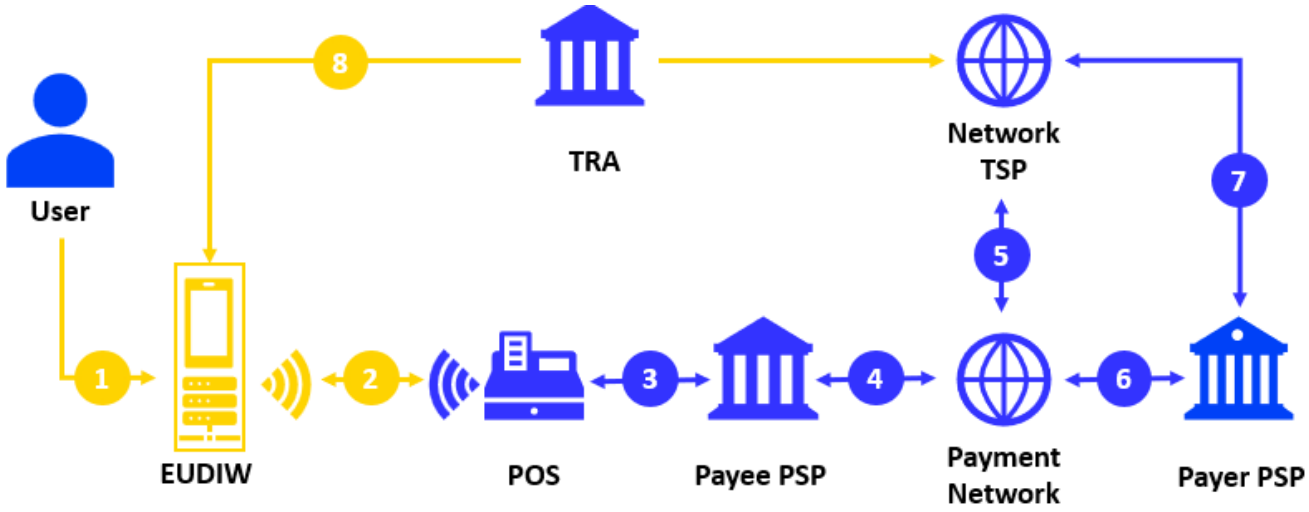
- User
- Merchant/payee
- Payer PSP (card issuer)
- Payee PSP (acquirer)
- POS terminal
- Payment network
- Payee PSP

EWC | Co-funded by the European Union

- EUDI Wallet Instance
- EUDI Wallet Provider
- Token Service Provider
- Token Requestor
- Token Requestor Aggregator

3.3 High-level Payment flows

3.3.1 Method A.1: Authenticated in-store payment with device-based EUDI Wallet



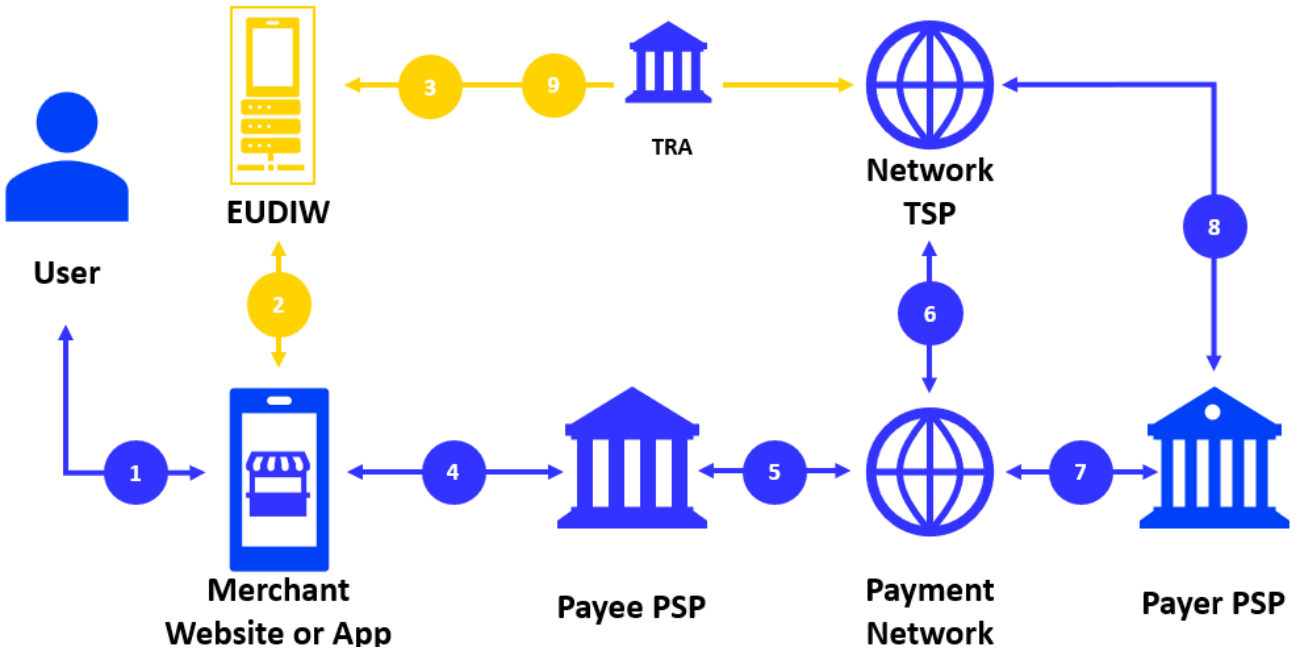
1. The user purchases goods at a store and chooses to pay with the EUDI Wallet app installed on the mobile device. The user opens it, logs on and selects the card to use for the transaction.
2. The user taps the mobile device at the merchant's Point of Sale (POS) terminal. The EUDI Wallet uses the payment keys stored on the mobile device to generate the payment cryptogram.
3. The POS terminal captures the token details and the payment cryptogram and sends an authorisation request to the payee PSP (acquirer) using the EMV contactless protocol ISO/IEC 14443.
4. The payee PSP forwards the authorisation request including the ARQC to the payment network (like Visa, Mastercard, etc.).
5. The payment network takes the token from the authorisation request and detokenises it with the Network TSP to retrieve the original card details.
6. The payment network then creates a new authorisation request with the original card details and routes it to the payer PSP (card issuer). The PSP checks the user's

EWC
Co-funded by the European Union

account and decides to either approve or decline the transaction. The payer PSP sends the response back through the same path to inform the merchant.

7. Optionally, the payer PSP can now (or at any other moment) connect with the TSP to change the state of the token (for example in case of suspected fraud).
8. The EUDI Wallet provider connects with the network TSP (via the TRA) to retrieve a new key for cryptogram generation if necessary (i.e. payment key can expire or reach a maximum number of transactions).

3.3.2 Method A.2: Authenticated online payment with device-based EUDI Wallet



1. The user purchases goods through a merchant's website or app, proceeds to the checkout page, and chooses to pay with the EUDI Wallet.
2. The merchant invokes the EUDI Wallet app installed in the mobile device. The user logs in the EUDI Wallet and selects the card for this checkout.
3. If the card is a Visa card, a cryptogram is obtained from the TSP (usually via the TRA). If the card is a Master Card, the EUDI Wallet uses the payment keys stored in the mobile device to generate the payment cryptogram for the transaction.
4. The merchant receives the token details and the payment cryptogram. We currently assume that this can be facilitated using OpenID for Verifiable Presentations. It then sends the authorisation request to its payee PSP.
5. The payee PSP forwards the authorisation request to the payment network (such as Visa, Mastercard, etc.).

EWC | Co-funded by the European Union

6. The payment network takes the token from the authorisation request and detokenises it with its network TSP to retrieve the original card details.
7. The payment network then creates a new authorisation request with the original card details and routes it to the payer PSP. The payer PSP checks the user's account and decides to either approve or decline the transaction. The payer PSP sends the response back through the same path to inform the merchant.
8. Optionally, the payer PSP can now (or at any other moment) connect with the TSP to change the state of the token (for example in case of suspected fraud).
9. If the card is a Master Card, the EUDI Wallet connects with the network TSP to retrieve a new key for cryptogram generation if necessary (i.e. payment key can expire or reach a maximum number of transactions).

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)

EWC | Co-funded by the European Union

- Tink (Sweden)
- Token ID (Netherlands)
- Visa (UK)
- Worldline (France)

Co-funded by the European Union