OID4VP for Payment Confirmation – Background

- The EWC is one of four consortia running Large Scale Pilots for the upcoming EU Digital Identity Wallets
- At EWC, we are investigating (among other topics) how EUDI Wallets can be used for payments
- eIDAS 2.0, Article 5f: “Where private relying parties (…) are required by (…) law to use strong user authentication (…) including in the areas of (…) banking, financial services, (…) those private relying parties shall (…) also accept European Digital Identity Wallets (…).”
- PSD2, Article 97 (2): “With regard to the initiation of electronic payment transactions (…) Member States shall ensure that (…) payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.”
- PSD2 RTS, Article 5 (1): “Where payment service providers apply strong customer authentication (…) they shall also adopt security measures that meet each of the following requirements:
  a) the payer is made aware of the amount of the payment transaction and of the payee;
  b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;
  c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;
  d) any change to the amount or the payee results in the invalidation of the authentication code generated.”

Co-funded by the European Union

OID4VP for Payment Confirmation – Requirements and Solution

- Use case: A customer instructs his/her bank to execute a payment transaction from his/her account
- The bank must ensure that:
  - The customer is the customer he/she claims to be and not someone else
  - The customer has seen the transaction details (amount and payee as minimum)
  - The customer has approved this very transaction (and not any other payment)
  - All of the above must be cryptographically verifiable
- The standard solution approach for this use case is a challenge-response pattern where the transaction details are included in the challenge
- OID4VP as it stands can help to authenticate the customer, but it lacks the capability to include *dynamic* information as credentials in the wallet are of a static nature
- We therefore support the proposed extension to introduce a transaction_data mechanism where the Relying Party can:
  - include dynamic information to be signed by the user and then returned to the RP and
  - articulate which key the user is supposed to use for this operation (as the user may have multiple and not all may be known to the RP).

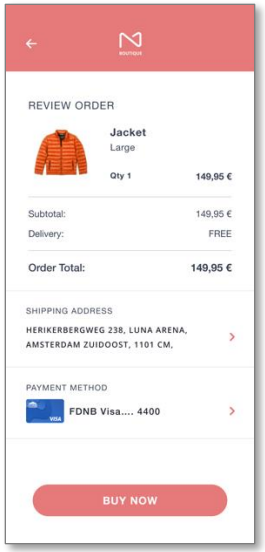
Sample User Experience

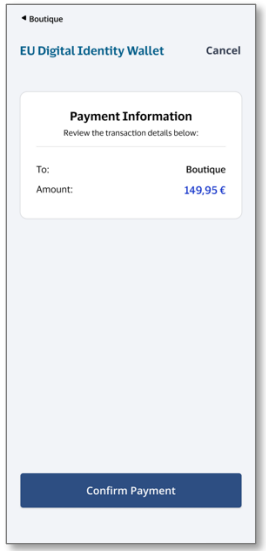
1) Using merchant app, user makes purchase using registered card.

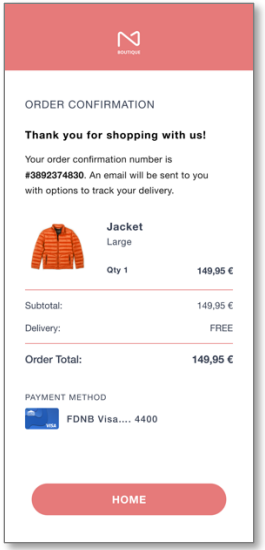
2) User authenticates to EUDI Wallet for the activity of payment confirmation.

3) User confirms payment.

4) Merchant app confirms successful transaction.







Co-funded by the European Union