Embedded Authentication Flow

1. **Identification & Verification (ID&V):**
   The customer submits their ID information to the TPP, who verifies their identity using a digital ID verification solution and additionally collects customer information using eKYC or another source. The ID information will be sent to the ASPSP.

2. **Customer Verification:**
   The customer chooses the ASPSP for account selection and access via TPP app. The ASPSPs verify the customer's identity, sending an SMS (OTP) and/or an email to the registered mobile number or email address of the customer based on the ID information received from the TPP.

3. **Device Binding:**
   Once verified by the ASPSPs, TPPs will limit the access to one device and link the device to a digital certificate that shall be passed to ASPSP in each API call.

4. **Selection of Accounts:**
   Upon successful verification a comprehensive list of the customer's existing accounts is presented. The customer can then conveniently select the specific accounts they wish to include as part of the Open Banking services.

5. **Utilizing Open Banking Services:**
   Following account selection, the customer gains access to the provided Open Banking services offered by the TPP for the selected accounts. For payment authorisation in case of PISP, ASPSPs can apply an additional authentication factor (which does not require the customer access the ASPSP’s website or app) such as an OTP.

6. **Consent Management:**
   The consent management remains unchanged, but consent approval will be embedded and not require the customer to be redirected to another webpage/app. However, ASPSPs must also provide the dashboard on their webpage or app.