1-SCA biometric authentication solution using a Mobile Bank application

Introduction to the biometric authentication solution for users of the **PSD2 PIS API**

Introduction

The original PSD2 solution for Netcompany Banking Service bank customers (end users) is based on a double (2) Strong Customer Authentication (2-SCA) solution, meaning that the end user (PSU) will have to authenticate themselves two times: The first time to give the Third Party Provider (TPP) consent to act on behalf of the end user, and the second time when signing a payment request.

This booklet introduces a new single SCA (1-SCA) biometric authen-tication solution, which enables a TPP to use Netcompany Banking Service's Mobile Bank* application as authentication device, like the MitID or the BankID app, to carry out a payment flow with only one authentication of the end user, hence the name: "1-SCA".

Should you have any questions regarding the authentication solution, you are welcome to send an e-mail to psd2support@sdc.dk

Table of Contents

In this booklet you will find an overall description of the 1-SCA biometric authentication solution, which will help you to understand:

*Note: The biometric authentication solution is not supported by the Swedish Netcompany Banking Service Banks.

The end user journey using the 1-SCA authentication solution

A potential shopping situation:

A 1-SCA authentication solution is especially applicable for buying situations where the focus for the end user is on the tasks performed in a TPP application, like shopping for shoes or wine. When the end user wants to pay for the item, he/she just needs to provide the relevant payment information and approve the payment by using the Mobile Bank application from the end user's Netcompany Banking Service Bank.
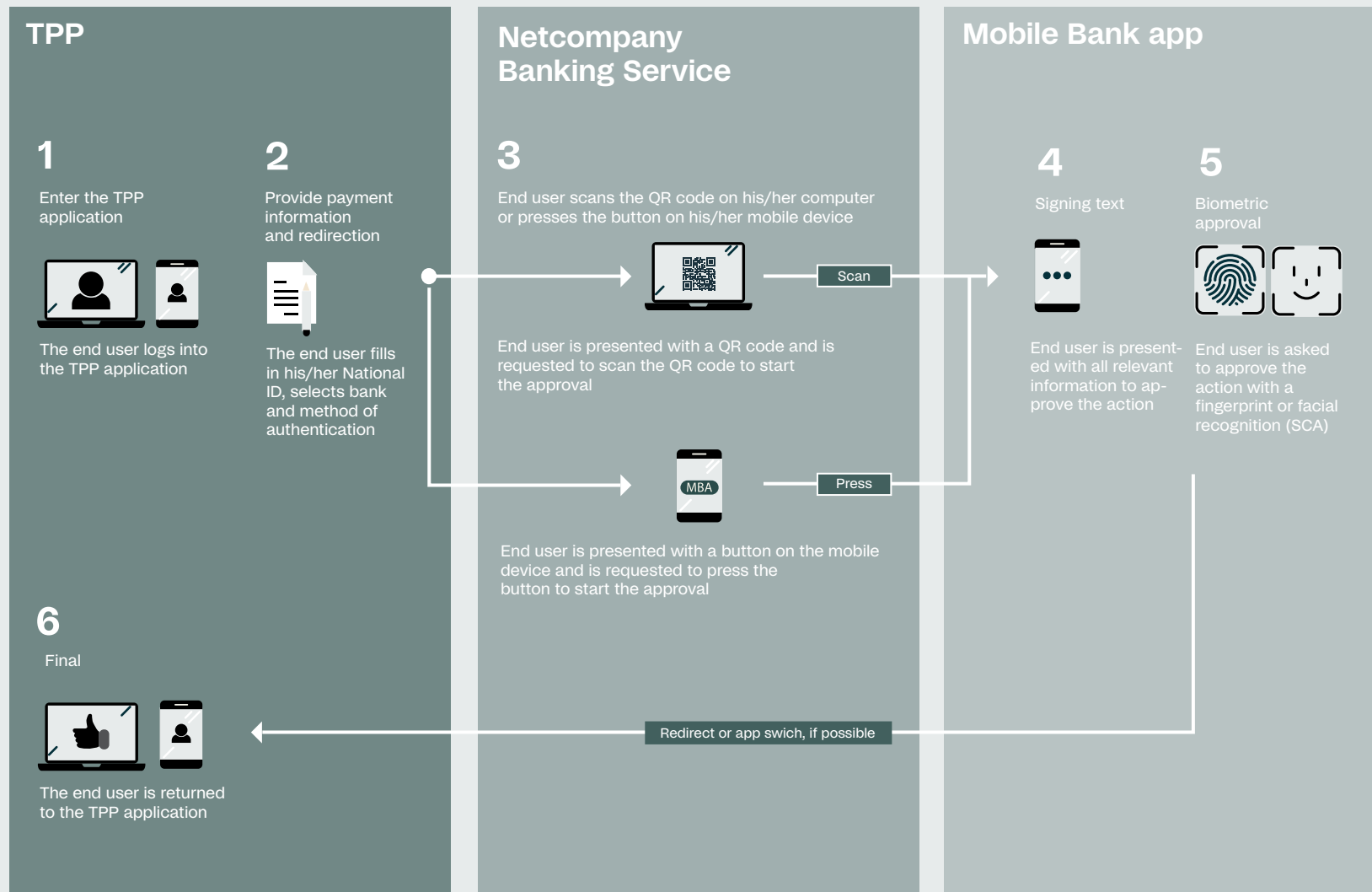
The figure on page 5 illustrates the end user journey for a payment initiation flow using the 1-SCA authentication solution. →

The end user journey proceeds as follows:

1 The end user enters/logs into the TPP application

2 The TPP displays a page where the end user provides the necessary information, such as sender account, recipient account, amount, payment date, and his/her national identification number

3 The TPP redirects the end user to Netcompany Banking Service, who displays either a QR code, if the flow is performed on a computer, or a button, if the flow is performed on a mobile device

4 The end user either scans the QR code or press the button, and the Mobile Bank app from the Netcompany Banking Service Bank will automatically open and display the payment data provided by the end user to the TPP (excluding the national identification number)

5 The end user can now approve the action with his/her fingerprint or by scanning his/her face

6 Netcompany Banking Service redirects the end user back to the TPP

This was a short description of the end user journey of the biometric authentication solution, but to utilise it, you will need to be onboarded as a TPP first.

Using the 1-SCA as authentication method

TPP

1
Enter the TPP application

The end user logs into the TPP application

2
Provide payment information and redirection

The end user fills in his/her National ID, selects bank and method of authentication

Netcompany Banking Service

3
End user scans the QR code on his/her computer or presses the button on his/her mobile device

Scan

End user is presented with a QR code and is requested to scan the QR code to start the approval

MBA

Press

End user is presented with a button on the mobile device and is requested to press the button to start the approval

Mobile Bank app

4
Signing text

End user is presented with all relevant information to approve the action

5
Biometric approval

End user is asked to approve the action with a fingerprint or facial recognition (SCA)

6
Final

The end user is returned to the TPP application

Redirect or app swich, if possible

What are the pre-requisites for utilising the 1-SCA authentication solution?

If you want to employ this 1-SCA solution, you must first onboard to Netcompany Banking Service's current 2-SCA solution to:

- Provide Netcompany Banking Service with your credentials and redirect URLs
- Receive client id's for accessing relevant Netcompany Banking Service banks
- Get access to the Netcompany Banking Service PSD2 Developer Portal
- Get access to the Netcompany Banking Service PSD2 APIs
- Use the 2-SCA solution to gain access to AIS content, if needed

If you have not already been onboarded, you can fill out the onboarding form on the PSD2-site.

Should you wish to access the test environment to test the token exchange process, please send a request to psd2support@sdc.dk

To utilise the 1-SCA solution, please provide Netcompany Banking Service with the following information:

Besides the information given during onboarding to the current 2-SCA solution, you also need to provide Netcompany Banking Service with the following to utilise the 1-SCA solution:

1   Your eIDAS QSealC certificate

The certificate must be sent to psd2support@sdc.dk in text format (Input Base64). Netcompany Banking Service will notify you as soon as your certificate has been stored in our backend.

In addition to the certificate you must provide:

2   An identification of the TPP calling Netcompany Banking Service's PSD2 APIs

The identification must consist of an URL using the "https" scheme and without any query or fragment components.
Please state like this: *Issuer string: https://servername.tppname.dk*

How the 1-SCA authentication solution works from a technical perspective

Besides being onboarded, you as a TPP also need to develop some code which can create a new JSON Web Token each time your end user (PSU) initiates a new payment. This is needed in order to leverage the technical set-up behind the 1-SCA payment initiation journey. Thus, the sequence diagram for a 1-SCA payment initiation flow looks like this:
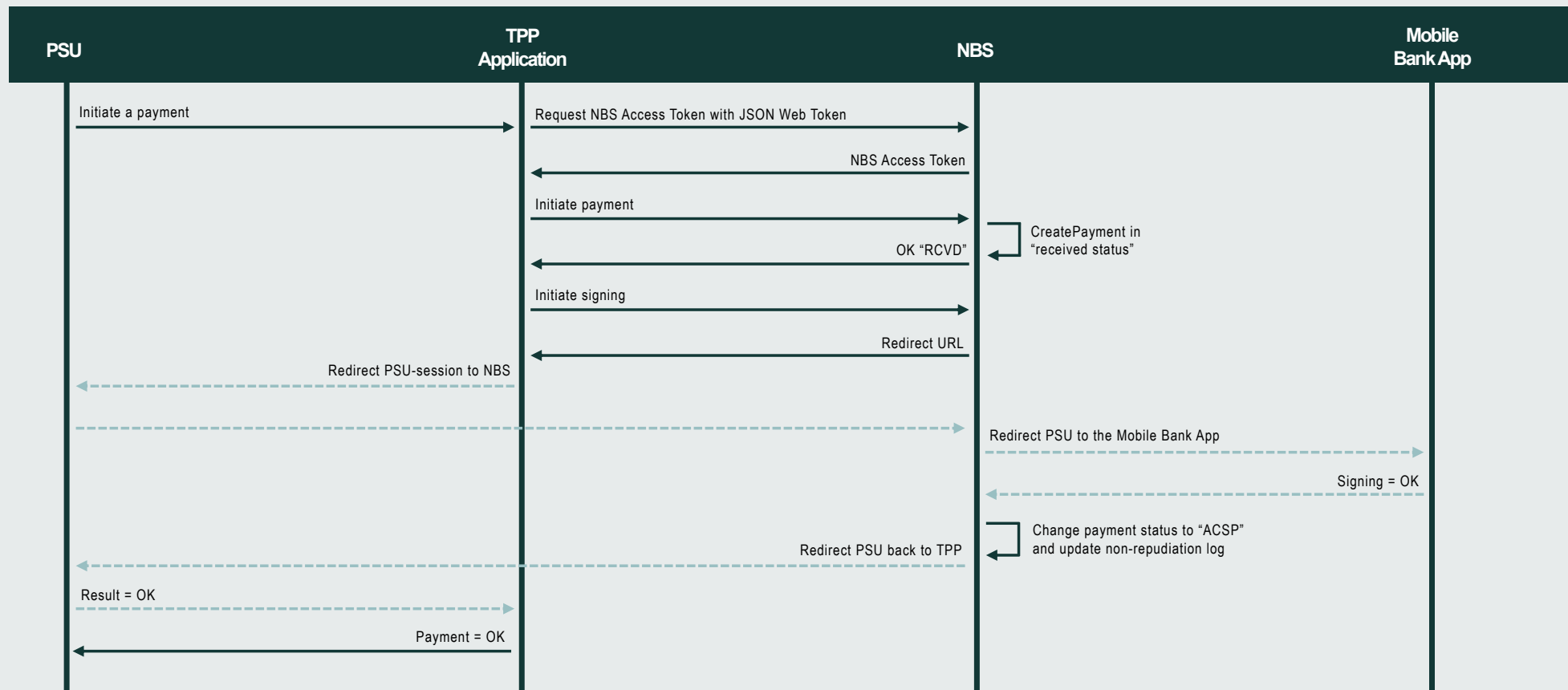
As illustrated, this is how the overall description of the technical flow will look like:

1. An end user requests the TPP to initiate a payment and provides all relevant information, including the end user's national identification number
2. The TPP calls the Netcompany Banking Service (NBS) endpoint with a JSON Web Token (JWT) as bearer token to request a "NBS Access Token", which follow the RFC-7523 standard. The JWT must be signed with the TPP's QSEAL eIDAS certificate
3. NBS validates the JWT token and issues a "NBS Access Token" (valid for 5 minutes), which is returned to the TPP

Note, that the following steps are the same as in the current 2-SCA solution:

4. The TPP calls the PSD2-operation "initiate Payment" with the "NBS Access Token"
5. If the provided information is accepted, NBS responds with an "RCVD" status (i.e., Received) and a unique "payment-ID" to the TPP
6. The TPP then calls NBS again to start the signing process
7. NBS responds by providing a redirect URL, which the TPP uses to direct the end user to the Mobile Bank app provided by a NBS Bank
8. The end user approves (signs) the payment using the Mobile Bank app provided by a NBS Bank
9. If the signing in the Mobile Bank app is successfull, NBS responds with an OK and redirects the end user to the TPP application
10. The payment is now in status "ACSP" (i.e., Accepted Settlement in Progress)

Concluding Remarks and Contact Information

This was a short introduction to the 1-SCA authentication solution for payment initiation through Netcompany Banking Service's PSD2 API. If you want to implement this solution, we recommend that you read the technical documentation, available on our Developer Portal, which you can access as an onboarded TPP.

Should you have any other questions regarding the authentication solution, you are welcome to send an e-mail to **psd2support@sdc.dk**

Netcompany
Banking Services