SCA Methods Guide

An overview of our available SCA methods and redirect flow

Contents

I. Introduction

In this guide you will find an overview of the Argenta SCA methods that are available for you to use. We offer all three of our SCA methods through our dedicated API platform: digipass, pin and Itsme. This document gives a description of the different methods.

For each request that requires SCA, you are asked to indicate a preferred method. However, just like on our own channels, the available methods are context dependent: not all methods may be available for all types of transactions and in all situations. Your preference will be taken into account to the extent that it is possible, both technically and within our business rules.

All our SCA methods follow the same OAuth 2.0 redirect flow, which ensures that you will not need to build a specific integration per method. In all cases, the customer will be redirected to our Authorization Server, where the customer is identified using one of our SCA methods. After authorization the customer will be redirected back to the TPP application with an authorization code. The TPP can use this code to retrieve an access / refresh token.

This document contains only a functional description of the SCA methods and redirect flow. For technical implementation details of the API's and how to select your preferred SCA method, please consult our Implementation Guide.

II. SCA Methods

1. Array of SCA Methods

When initiating a request on our API's and multiple SCA methods are available, the response will contain an array object called **scaMethods**. You can either indicate a preference for one of the methods, or choose no preference. Below is an example of this scaMethods response:

```
{
    "scaMethods": [
        {
            "name": "Digipass",
            "authenticationType": "DIGIPASS",
            "explanation": " Authenticate using an Argenta bank card and digipass card reader",
            "authenticationMethodId": "DIGIPASS"
        },
        {
            "name": "Pin",
            "authenticationType": "PIN",
            "explanation": " Authenticate using the Argenta mobile banking app",
            "authenticationMethodId": "PIN"
        },
        {
            "name": "Itsme",
            "authenticationType": "ITSME",
            "explanation": " Authenticate using the Belgian Itsme identity app",
            "authenticationMethodId": "ITSME"
        },
        {
            "name": "No preference",
            "authenticationType": "NO_PREFERENCE",
            "explanation": " No specific authentication method preferred",
            "authenticationMethodId": "NO_PREFERENCE"
        }
    ],
```

2. Digipass

The Digipass method is our default SCA method, which is available for all transaction types and across all devices. It requires the customer to authenticate with his **Argenta bank card and Argenta Digipass card reader**. The customer is redirected to an Argenta webpage that contains the details of the transaction, and a digipass signing screen that resembles our Internet Banking. The customer can choose his/her preferred language (NL/FR/EN) on the screen itself. The default language will be based the browser language of the customer.

Details of the transaction

Do you give **PSDBE-PIS-123456** permission to execute the following transaction?
Amount: 123.45 EUR
From: BE249973170817438
To: Mr. Apples BE19000000001212
Communication: Free text

Confirm your transaction

My cardnumber:

____ ____ ____ ____   ☐ Save my cardnumber

Put your debit card into your Digipass and push (M2)

Enter your pin code and push (OK)

Enter the challenge 56431518 into your Digipass and push (OK)
Enter the challenge 12345190 into your Digipass and push (OK)

Push again on (OK)

Enter the response code here:

· · · · · · · ·

Login

⊗ CANCEL

3. PIN

The PIN method uses the Argenta Mobile App to authenticate transactions. This means that the customer having the Argenta App installed on the device being used is a precondition for using this authentication method, and that this method is not available on non-mobile (Android or iOS) devices. When choosing PIN as your preferred method on a non-mobile device, the chosen preference will be treated as invalid and defaults to no preference (see section 5: No preference).

Additionally, this method is not allowed for financial transactions that exceed certain limits. In case a limit is exceeded, the customer will automatically be offered an alternative SCA method within the Argenta App.

Using this authentication method will redirect the customer to the Argenta App. The app shows the details of the transaction and allows the customer to authenticate using either the **pincode or biometrics** of his/her Argenta App. The language is based on the language the customer uses in the app.
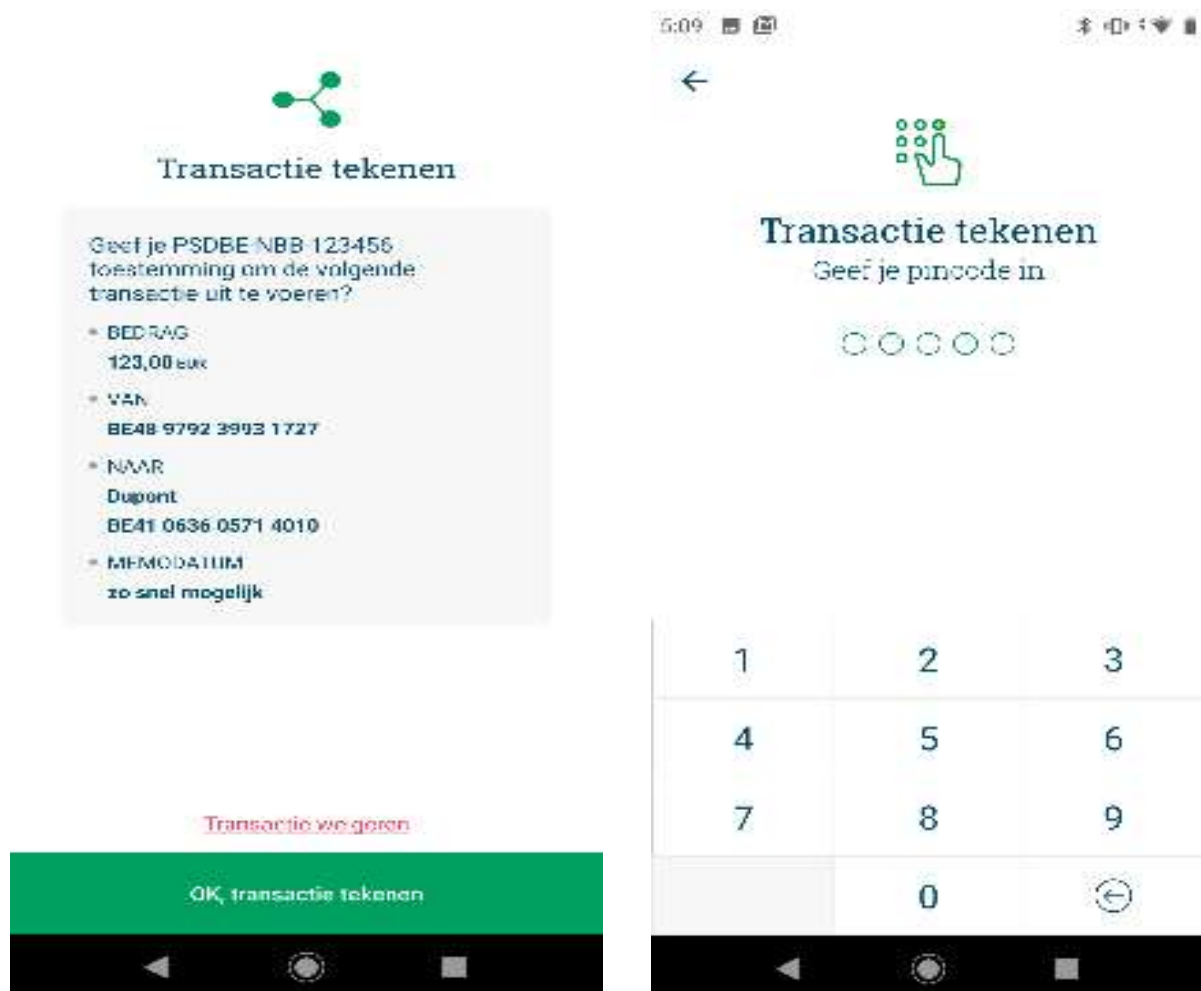
4. Itsme

The Itsme method makes use of the Itsme app. This means that the customer having installed and registered the Itsme app is a precondition for being able to use this authentication method. The customer will be redirected, via Argenta, to the Itsme app.
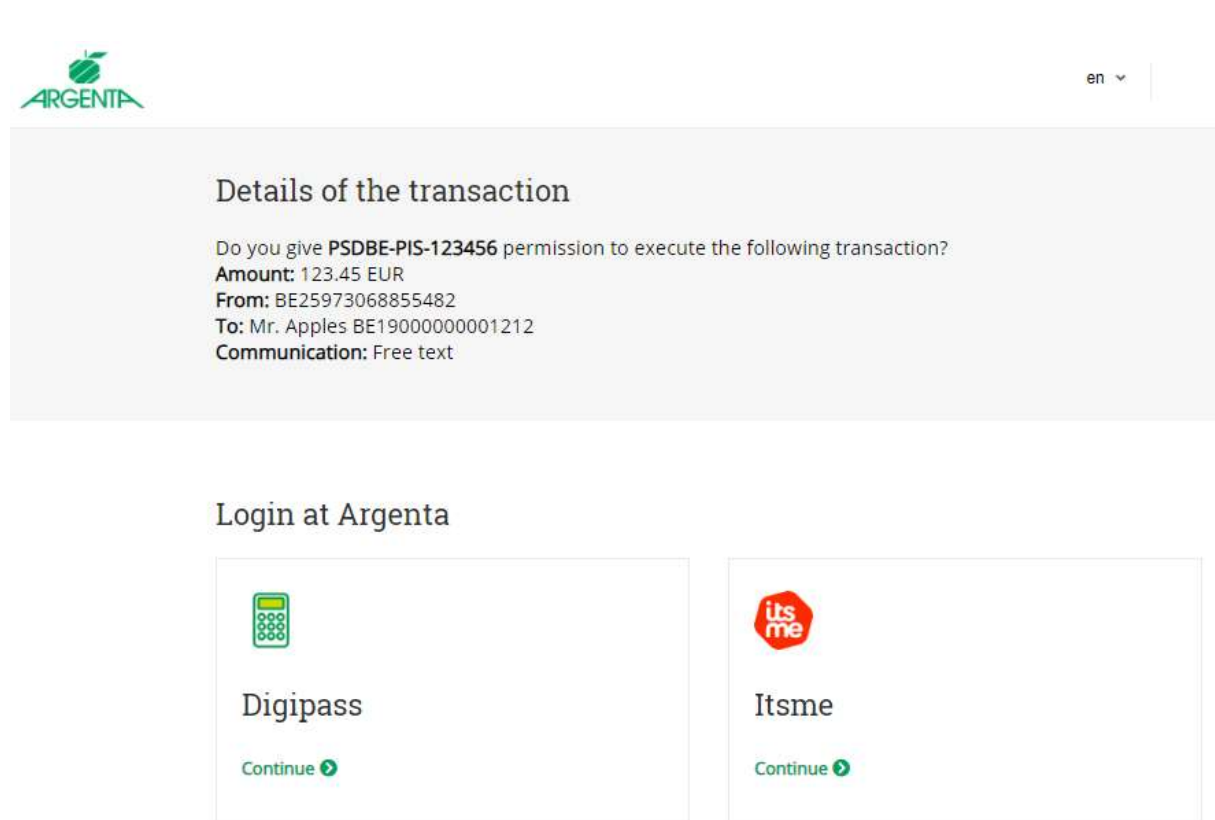
The Itsme app shows the details of the transaction and allows the user to authenticate using either the **pincode or biometrics** of his/her Itsme app. The language is based on the browser language of the customer and the language settings of the Itsme app.
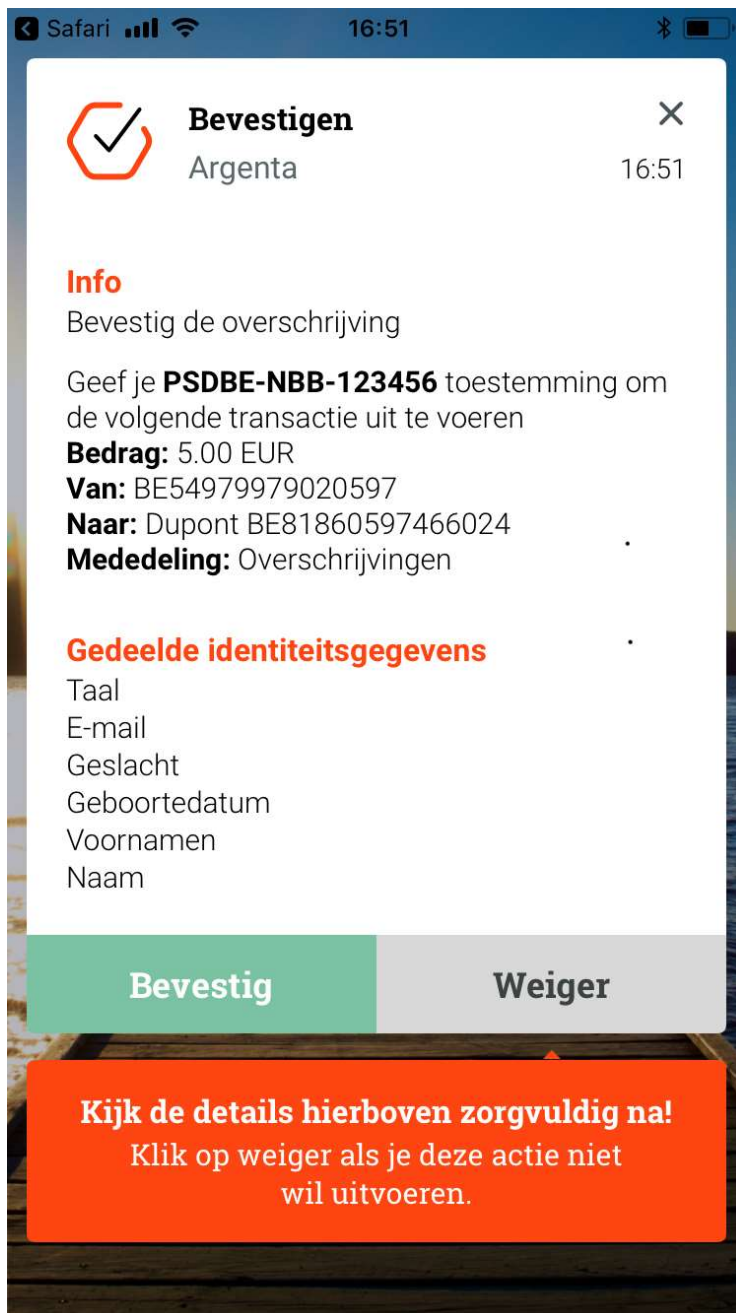
5. No Preference

When selecting the no_preference method, the customer will be redirected to an SCA method selection page at Argenta. Here the customer will be able to choose from the available SCA methods, whereby the available methods are determined on the basis of the device the customer is using.

When the customer is using a desktop computer, only Digipass and Itsme are offered as choices.

When the customer is using a mobile device (Android or iOS), a choice of all three SCA methods is offered:

Here the customer can select whichever SCA method he/she prefers by clicking the corresponding button. The customer will then be redirected to the chosen SCA method.

III. OAuth 2.0 Redirect Flow

All our SCA methods follow the same OAuth 2.0 redirect flow. The flow contains nested internal redirects which all follow the same basic logic. For any of our SCA methods, the flow is the following:

1. TPP redirects customer to a public URL at our API platform

2. The API platform redirects to our Authorization Server

3. Customer chooses SCA method and is redirected

4. Customer authenticates the request with SCA

6. Authorization server redirects back to API platform

6. API Platform validates the initial request

7. API Platform redirects the customer back to the callback URL of the TPP with an authorization code (to be exchanged for an access token)