La CommunautéBPCE
INNOVATION, DATA ET DIGITAL

Digital services

# PSD2 Strong Customer Authentication

## Analysis : **FIDO2 keys** as a replacement for **CAP** (Chip Authentication Program) **readers**

- May 2022

GROUPE BPCE

**01** Introduction

**02** BPCE Specificities

**03** Typical Customer Journey

**04** Our concerns about FIDO2 > PSD2 SCA Requirements

**05** Questions

# 01 Introduction

# About BPCE

## A French Banking Group

*Source : https://groupebpce.com/en/the-group/profile*

# European regulations for banking and payment

## PSD2 : Payment Services Directive – Revised version

### PSD2 in brief

- Member states of the European Union need to comply to the EU PSD2 requirements since January 2018.
- The rules aim to :
  - better protect customers when they bank online – through **Strong Customer Authentication**
  - promote the development and use of innovative banking and payment services – through **Open Banking**

### Focus : Strong Customer Authentication (SCA)

- **Identification** : recognizing the customer concerned by an operation
- **Authentication** : making sure that the user behind the operation is in fact the customer – by one of the following factors :
  - Inherence > (biometric) properties of the customer
  - Knowledge > (secret) information known by the customer
  - Possession > (personal) physical belonging of the customer
- **Strong Authentication** : combining at least two of the three factors to authenticate the user

# Our understanding of Strong Customer Authentication

## In brief : PSD2 SCA Requirements

### PSD2 rules apply for every online / remote banking operation, be it on :

- Internet banking (web access) and Mobile banking (smartphone application) ;
- Phone banking (call-centers) ;
- E-commerce websites (3DS online payments) ; etc.

### Operations concerned by SCA requirements

✓ **1 Connection / Sign-in to online services**

When the customer logs-in to his/her **internet banking** – on web interface or mobile application

- A strong authentication is required every 90 days or on a new device

✗ **2 Validation of a sensitive operation**

On remote banking (internet or phone) : when the customer initiates an **operation** classified as « **sensitive** » by PDS2.

- Examples : adding a new payee for bank transfers ; initiating a bank transfer to someone else…

✓ **3 Validation of an online payment**

When the customer makes an **online payment**, either :

- With his/her **card** – through 3DS (MasterCard or Visa) or ;
- By **instant payment** – through a Third-Party Provider (known as a “Payment Initiating Service Provider”).

# 02 BPCE Specificities

# Snapshot of BPCE Context

## Authentication means

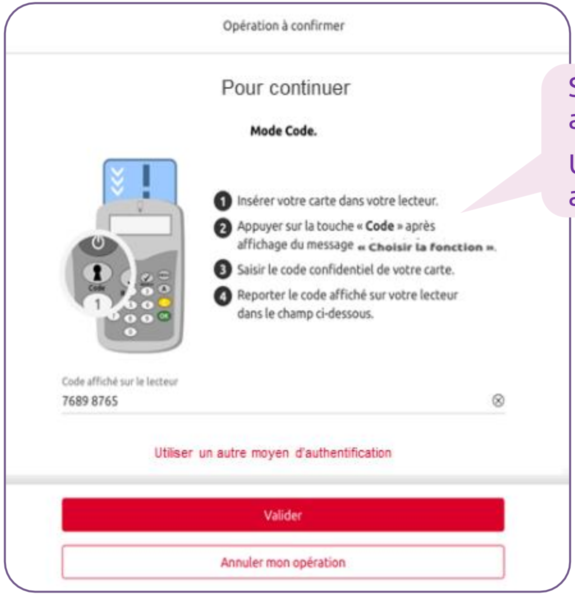
- **Summary of some (not all) authentication means that we propose to our customers**
  - Some authentication means are considered « **simple** » (or weak)
    - They need to be **combined** to provide a **strong authentication**
  - Some authentication means are considered « **strong** » and do not need to be combined for SCA
    - They combine **multiple factors** (inherence, possession or knowledge) in **one single means**

| Authentication means | Type<br>(simple / strong) |
|---|---|
| Password | Simple |
| OTP sent by SMS | Simple |
| **Sécur'Pass** : **In-app** notification and validation (on registered device) | **Strong** |
| **CAP reader** and card | **Strong** |
| Password **+** OTP SMS | **Strong** |

Our focus for today's presentation and discussions

# CAP-reader use cases

## In brief : The 2 operating modes of the CAP card reader



Opération à confirmer

Pour continuer

**Mode Code.**

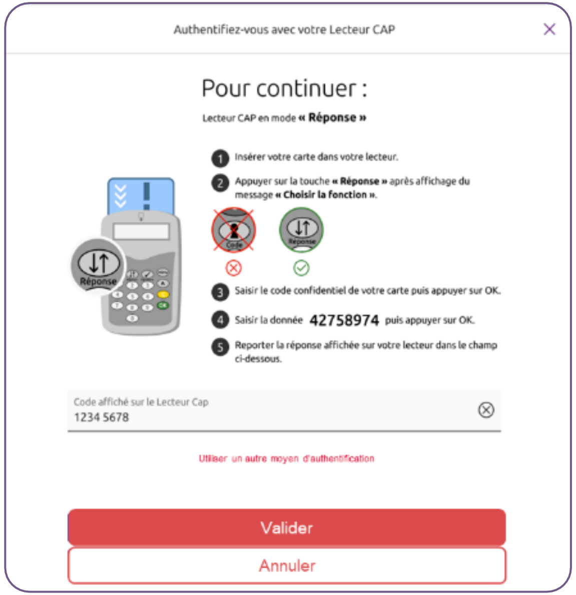
1. Insérer votre carte dans votre lecteur.
2. Appuyer sur la touche « **Code** » après affichage du message **« Choisir la fonction »**.
3. Saisir le code confidentiel de votre carte.
4. Reporter le code affiché sur votre lecteur dans le champ ci-dessous.

Code affiché sur le lecteur: 7689 8765

Steps to generate an authentication code

Used in combination with a chip-based card

*evolution*



Authentifiez-vous avec votre Lecteur CAP

Pour continuer :

Lecteur CAP en mode **« Réponse »**

1. Insérer votre carte dans votre lecteur.
2. Appuyer sur la touche **« Réponse »** après affichage du message **« Choisir la fonction »**.
3. Saisir le code confidentiel de votre carte puis appuyer sur OK.
4. Saisir la donnée **42758974** puis appuyer sur OK.
5. Reporter la réponse affichée sur votre lecteur dans le champ ci-dessous.

Code affiché sur le Lecteur Cap: 1234 5678

### Code mode

Unique authentication code generated randomly – used as an OTP to validate an operation

**Not PSD2 compliant** – for Remote banking "sensitive operations", as there is no dynamic linking

### Response mode

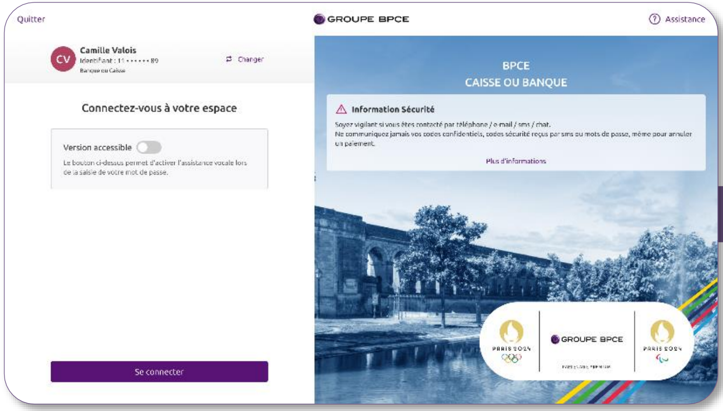
Unique authentication code generated **in response to a server code** – used as an OTP to validate an operation

**PSD2 compliant** – as there is a pair of unique codes (one identifying the transaction and one the authentication)

# 03 Typical Customer Journey

# Customer Journey : Adding a new payee (1/3)

## Steps : Log-in (id) > Log-in (password) > Internet banking home page (Accounts summary)



Camille Valois
Identifiant : 11 • • • • • • 89
Banque ou Caisse

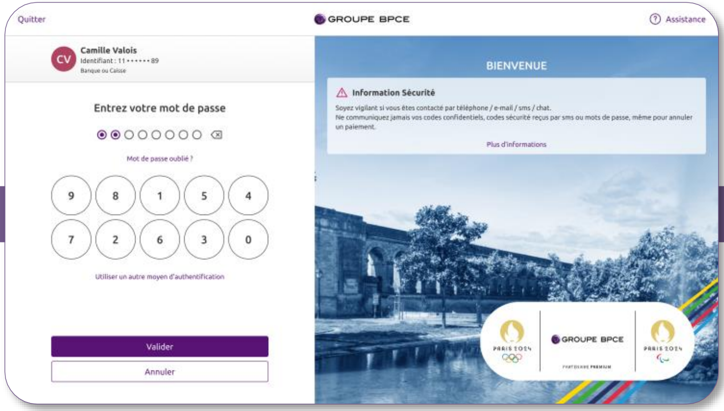
Connectez-vous à votre espace

Version accessible

Le bouton ci-dessus permet d'activer l'assistance vocale lors de la saisie de votre mot de passe.

**Information Sécurité**

Soyez vigilant si vous êtes contacté par téléphone / e-mail / sms / chat.
Ne communiquez jamais vos codes confidentiels, codes sécurité reçus par sms ou mots de passe, même pour annuler un paiement.

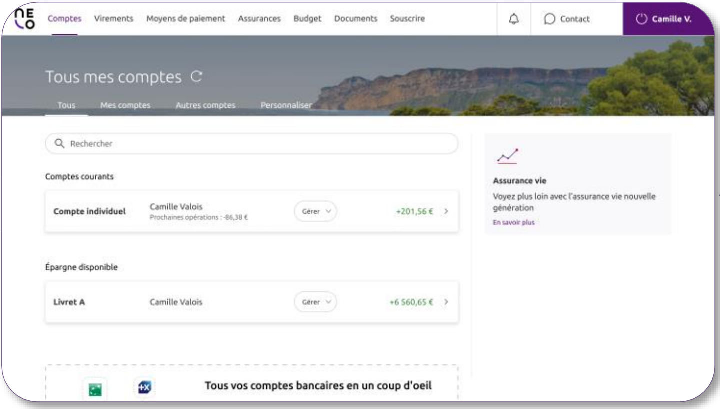


Camille Valois
Identifiant : 11 • • • • • • 89
Banque ou Caisse

Entrez votre mot de passe

**Information Sécurité**

Soyez vigilant si vous êtes contacté par téléphone / e-mail / sms / chat.
Ne communiquez jamais vos codes confidentiels, codes sécurité reçus par sms ou mots de passe, même pour annuler un paiement.



Tous mes comptes

Comptes courants

| | | |
|---|---|---|
| Compte individuel | Camille Valois<br>Prochaines opérations : -86,38 € | +201,56 € |

Épargne disponible

| | | |
|---|---|---|
| Livret A | Camille Valois | +6 560,65 € |

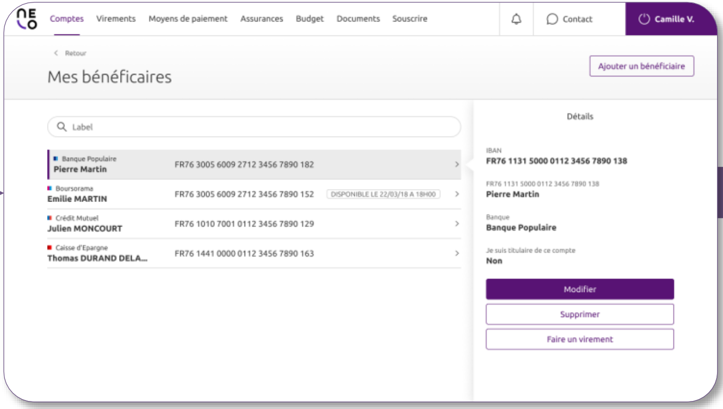
**Assurance vie**

Voyez plus loin avec l'assurance vie nouvelle génération

Tous vos comptes bancaires en un coup d'oeil

# Customer Journey : Adding a new payee (2/3)

## Steps : Bank transfers > List of payees > Add a new payee



Mes bénéficaires

Label

| | | | |
|---|---|---|---|
| Banque Populaire<br>**Pierre Martin** | FR76 3005 6009 2712 3456 7890 182 | | › |
| Boursorama<br>**Emilie MARTIN** | FR76 3005 6009 2712 3456 7890 152 | DISPONIBLE LE 22/03/18 A 18H00 | › |
| Crédit Mutuel<br>**Julien MONCOURT** | FR76 1010 7001 0112 3456 7890 129 | | › |
| Caisse d'Epargne<br>**Thomas DURAND DELA...** | FR76 1441 0000 0112 3456 7890 163 | | › |

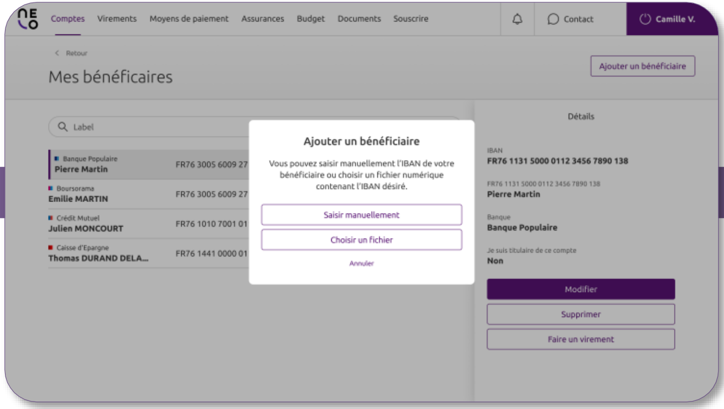
Détails

IBAN
**FR76 1131 5000 0112 3456 7890 138**

FR76 1131 5000 0112 3456 7890 138
**Pierre Martin**

Banque
**Banque Populaire**

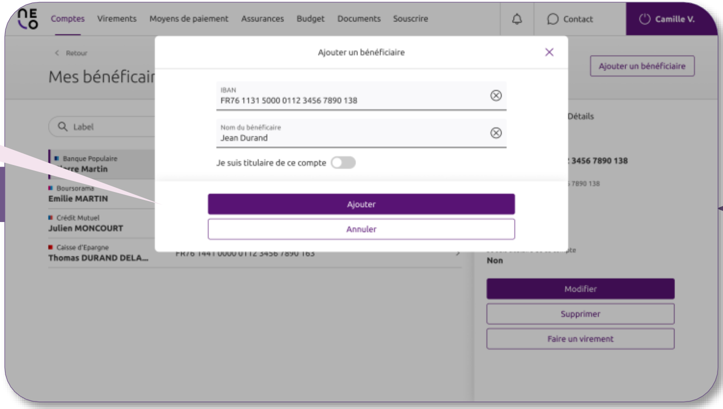
Je suis titulaire de ce compte
**Non**



Mes bénéficaires

Ajouter un bénéficiaire

Vous pouvez saisir manuellement l'IBAN de votre bénéficiaire ou choisir un fichier numérique contenant l'IBAN désiré.



Ajouter un bénéficiaire

IBAN
FR76 1131 5000 0112 3456 7890 138

Nom du bénéficiaire
Jean Durand

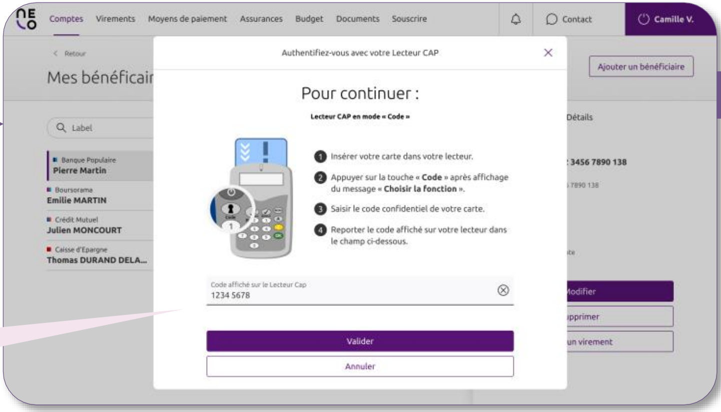
Je suis titulaire de ce compte ○

At this point, an **SCA** is required to confirm the user input

# Customer Journey : Adding a new payee (3/3)

## Steps : SCA (2 scenarios) > Confirmation of operation (new payee added)

Scenario 1 : **CAP reader**



Authentifiez-vous avec votre Lecteur CAP

Pour continuer :

**Lecteur CAP en mode « Code »**

1. Insérer votre carte dans votre lecteur.
2. Appuyer sur la touche « **Code** » après affichage du message « **Choisir la fonction** ».
3. Saisir le code confidentiel de votre carte.
4. Reporter le code affiché sur votre lecteur dans le champ ci-dessous.

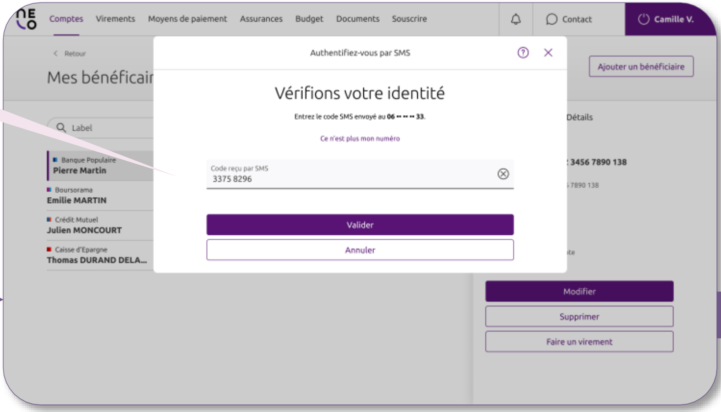
Code affiché sur le Lecteur Cap: 1234 5678

Valider

Annuler

**OR**

Scenario 2 : OTP **SMS**



Authentifiez-vous par SMS

Vérifions votre identité

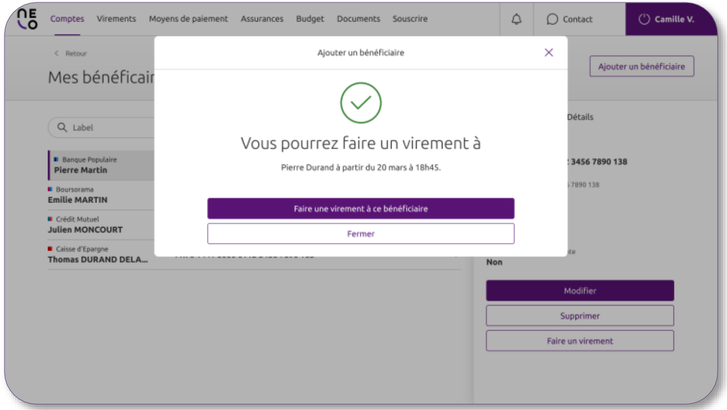
Entrez le code SMS envoyé au **06 •• •• •• 33**.

Ce n'est plus mon numéro

Code reçu par SMS: 3375 8296

Valider

Annuler



Ajouter un bénéficiaire

Vous pourrez faire un virement à

Pierre Durand à partir du 20 mars à 18h45.

Faire une virement à ce bénéficiaire

Fermer

# 04 PSD2 SCA requirements and FIDO2 specifications

# PSD2 and Security Requirements regarding SCA

## What you see is what you sign and Dynamic Linking

**The following requirements apply to both user validations :**

- Sensitive operation on Internet banking
- Online payments (Card-based or instant payment) on e-commerce websites

## What you see is what you sign (WYSIWYS)

- The client needs to be able to see on-screen the (details of the) operation he is about to validate / authenticate

## Dynamic Linking

- Dynamic linking - in a PSD2 context - requires an "authentication code", unique to each transaction, to be transferred together with the amount and recipient of the payment through every step of the payment and authentication process.

# FIDO2 specifications

## FIDO2 key as the best new means, with some limitations

- **Thanks to the Secure Payment Confirmation extension to FIDO2**
  - 3DS online card payment on e-commerce websites – can be authorised with FIDO2 devices in full PSD2-compliancy
- **Our concerns : Validating / authorising sensitive operations on Internet Banking**
  - What you see is what you sign
  - Dynamic Linking
- **Examples of sensitive operations requiring SCA for user validation**

| Operation | Details |
|---|---|
| Transfers > Adding a new payee | Name, IBAN of new payee |
| Transfers > Transfer to a third-party account | Amount, IBAN, date |
| Card management > PIN preview | Card (or card type) |
| Card management > Changing payment threshold | Card (or card type), previous and new thresholds |
| Card management > Apple Pay in-app provisioning | Card (or card type), date |

# 05 Questions / remarques