# Authentic 2 - Development #69890

## custom_user : récupération du compte par envoi d'un code au numéro vérifié lorsque le mot de passe a été oublié par l'usager

05 octobre 2022 08:39 - Paul Marillonnet

| | | | |
|---|---|---|---|
| **Statut:** | Fermé | **Début:** | 05 octobre 2022 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | Paul Marillonnet | **% réalisé:** | 0% |
| **Catégorie:** | | **Temps estimé:** | 0:00 heure |
| **Version cible:** | | | |
| **Patch proposed:** | Oui | **Planning:** | Non |

**Description**

Dans #69223 on prévoit une séquence d'envoi d'un code de vérification du numéro de téléphone de l'usager à l'enregistrement.
Il faudrait une séquence similaire pour amener à l'écran de redéfinition du mot de passe, lorsque celui-ci a été oublié par l'usager.

**Demandes liées:**

| | | |
|---|---|---|
| Lié à Publik - Development #49212: Création de compte avec un numéro de télép... | **En cours** | **01 octobre 2021** |

### Révisions associées

**Révision cc443d7b - 04 mai 2023 14:51 - Paul Marillonnet**

models: sms code adjustments for password reset (#69890)

**Révision 45bc870c - 04 mai 2023 14:51 - Paul Marillonnet**

utils/sms: add password lost sms code recovery utils (#69890)

**Révision 9de50d40 - 04 mai 2023 14:51 - Paul Marillonnet**

forms/passwords: add phone field (#69890)

**Révision af8adcef - 04 mai 2023 14:51 - Paul Marillonnet**

views: handle phone input on pw reset view (#69890)

**Révision ba955051 - 04 mai 2023 14:51 - Paul Marillonnet**

provide generic input code logic (#69890)

Suited to both registration & password-change actions.

**Révision 6821c6d4 - 04 mai 2023 15:10 - Paul Marillonnet**

translation update (#69890)

### Historique

**#1 - 05 octobre 2022 08:39 - Paul Marillonnet**

*- Lié à Development #49212: Création de compte avec un numéro de téléphone mobile ajouté*

**#2 - 12 décembre 2022 10:40 - Paul Marillonnet**

*- Statut changé de Nouveau à En cours*

*- Assigné à mis à Paul Marillonnet*

C'était bloqué par #69223 pour la partie challenge de vérification du numéro de téléphone par envoi d'un code, maintenant validée. Je peux avancer ici.

**#3 - 17 janvier 2023 15:53 - Paul Marillonnet**

*- Fichier 0005-provide-generic-input-code-logic-69890.patch ajouté*

*- Fichier 0004-views-handle-phone-input-on-pw-reset-view-69890.patch ajouté*

*- Fichier 0003-forms-passwords-add-phone-field-69890.patch ajouté*

*- Fichier 0002-utils-sms-add-password-lost-sms-code-recovery-utils-.patch ajouté*

*- Fichier 0001-models-sms-code-adjustments-for-password-reset-69890.patch ajouté*

*- Statut changé de En cours à Solution proposée*

*- Patch proposed changé de Non à Oui*

0001 les modifications sur le modèle SMSCode, pour y inclure :
· le lien vers l'utilisateur émetteur de la demande,
· le flag pour indiquer que le code qui est créé est faux, ce qui permet de poursuivre la tentative de changement de mot de passe même lorsqu'aucun compte n'est trouvé (et donc ne pas révéler cette absence de compte connu pour le numéro saisi).

0002 les utilitaires d'envoi de SMS de changement de mot de passe.
0003 l'ajout du champ de téléphone au formulaire de demande de changement de mot de passe.
0004 pour le traitement de ce numéro de téléphone si saisi dans le formulaire de demande de changement de mot de passe.
0005 pour l'adaptation de la vue de saisie du code reçu (qui servait pour l'instant uniquement à la création de compte) et la validation du changement de mot de passe.

#### #4 - 27 février 2023 10:19 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> · le flag pour indiquer que le code qui est créé est faux, ce qui permet de poursuivre la tentative de changement de mot de passe même lorsqu'aucun compte n'est trouvé (et donc ne pas révéler cette absence de compte connu pour le numéro saisi).

Je n'ai juste pas compris ce point, on a pas ça pour les mails qu'est-ce qui change ici ?

#### #5 - 27 février 2023 16:43 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Paul Marillonnet a écrit :
>
> > · le flag pour indiquer que le code qui est créé est faux, ce qui permet de poursuivre la tentative de changement de mot de passe même lorsqu'aucun compte n'est trouvé (et donc ne pas révéler cette absence de compte connu pour le numéro saisi).
>
> Je n'ai juste pas compris ce point, on a pas ça pour les mails qu'est-ce qui change ici ?

Parce que pour les emails, pour ne pas donner d'indication sur l'existence ou non du compte dont on souhaite récupérer le mot de passe, il suffit de dire "Ok, si le compte existe pour cette adresse, un courriel de ré-initialisation a été envoyé à cette adresse".

Pour la récupération par num de tél, on peut aussi dire la même chose "Si un compte existe pour ce num alors un code a été envoyé à été envoyé par SMS à ce numéro", mais il faut tout de même basculer directement sur le formulaire de saisie (toujours dans l'idée qu'on ne révèle pas si le compte existe ou non), et pour ce faire il faut générer un jeton. On stocke toutefois l'information que ce jeton est faux, pour se simplifier la vie.

#### #6 - 30 mars 2023 16:58 - Benjamin Dauvergne

Toujours pas compris, pourquoi faut-il créer un faux code ? Si quelqu'un n'est pas dans la base soit on envoie rien soit comme pour les mails on envoie un SMS qui dit "vous n'avez pas de compte, pour en créer un cliquez ici.". Vu le coût des SMS je dirai bien de ne rien envoyer.

PS: c'est dans ces cas là que le système inverse ou ce serait les gens qui nous enverraient un code depuis leur mobile sur un numéro dédié serait plus pratique, c'est gratuit, on peut en faire des liens[1] sur les téléphones, ça valide que la personne possède bien le numéro et nous permet d'afficher immédiatement "Vous n'avez pas de compte, vous en voulez un ?".

[1]: https://www.rfc-editor.org/rfc/rfc5724

#### #7 - 03 avril 2023 08:54 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Toujours pas compris, pourquoi faut-il créer un faux code ? Si quelqu'un n'est pas dans la base soit on envoie rien soit comme pour les mails on envoie un SMS qui dit "vous n'avez pas de compte, pour en créer un cliquez ici.". Vu le coût des SMS je dirai bien de ne rien envoyer.

Actuellement dans la série de commits on envoie rien, juste on génère une URL opaque comme si le numéro était connu d'a2, cette URL présente un formulaire de saisie du "code que vous avez reçu par SMS, si ce compte existe", tout en sachant pertinemment qu'il n'y a eu ni code ni SMS. C'est ce que je pense être le miroir de ce qu'on a déjà avec les emails, i.e. ne pas faire du formulaire de mot de passe oublié un oracle sur l'existence des comptes.

#### #8 - 03 avril 2023 09:06 - Paul Marillonnet

*- Statut changé de Solution proposée à En cours*

Vu en privé avec Benj' : je vais rebaser et créer une PR.

#### #9 - 03 avril 2023 14:28 - Robot Gitea

Paul Marillonnet (pmarillonnet) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/31
- Titre : WIP:  custom_user  : récupération du compte par envoi d'un code au numéro vérifié lorsque le mot de passe a été oublié par l'usager ( #69890)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/31/files

#### #10 - 03 avril 2023 14:51 - Robot Gitea

*- Statut changé de En cours à Solution proposée*

#### #11 - 24 avril 2023 18:07 - Robot Gitea

*- Statut changé de Solution proposée à Solution validée*

Benjamin Dauvergne (bdauvergne) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/31

#### #12 - 24 avril 2023 18:08 - Robot Gitea

*- Statut changé de Solution validée à En cours*

Benjamin Dauvergne (bdauvergne) a relu et demandé des modifications sur une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/31

#### #13 - 04 mai 2023 14:31 - Robot Gitea

*- Statut changé de En cours à Solution proposée*

#### #14 - 04 mai 2023 14:31 - Robot Gitea

*- Statut changé de Solution proposée à Solution validée*

Benjamin Dauvergne (bdauvergne) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/31

#### #15 - 04 mai 2023 15:06 - Robot Gitea

*- Statut changé de Solution validée à Résolu (à déployer)*

Paul Marillonnet (pmarillonnet) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/31
- Titre : custom_user  : récupération du compte par envoi d'un code au numéro vérifié lorsque le mot de passe a été oublié par l'usager (#69890)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/31/files

#### #16 - 04 mai 2023 17:14 - Transition automatique

*- Statut changé de Résolu (à déployer) à Solution déployée*

#### #17 - 09 juillet 2023 04:42 - Transition automatique

Automatic expiration

### Fichiers

| | | | |
|---|---|---|---|
| 0005-provide-generic-input-code-logic-69890.patch | 16,6 ko | 17 janvier 2023 | Paul Marillonnet |
| 0004-views-handle-phone-input-on-pw-reset-view-69890.patch | 7,62 ko | 17 janvier 2023 | Paul Marillonnet |
| 0003-forms-passwords-add-phone-field-69890.patch | 7,52 ko | 17 janvier 2023 | Paul Marillonnet |
| 0002-utils-sms-add-password-lost-sms-code-recovery-utils-.patch | 4,83 ko | 17 janvier 2023 | Paul Marillonnet |
| 0001-models-sms-code-adjustments-for-password-reset-69890.patch | 3,62 ko | 17 janvier 2023 | Paul Marillonnet |