

Your guide to using the Self Service Portal to set your Passcodes and renew your Smartcard certificates



A joint publication by:



NHS
Connecting for Health

The Self Service Portal

The Self Service Portal enables you to reset your Smartcard Passcodes at any time and renew your Smartcard certificates when prompted to.

1 Passcodes

Passcodes and certificates are automatically checked every time you authenticate to the Spine, and you are warned when they are due for renewal or have to be renewed.

You can, however, reset your Passcodes at any time and it is recommended you do so at regular intervals.

When you were registered to use the Spine, you were requested to set your Smartcard Passcode. You may also have set an Account Recovery Passcode and/or Verification Passcode. The purpose of each Passcode is as follows:

- **Smartcard Passcode** enables you to authenticate to the NHS CRS. This Passcode must be 4-8 characters in length, preferably alphanumeric and a mixture of upper/lower case.

- **Account Recovery Passcode** is used by the Registration Authority to verify the identity of any user who makes a request for assistance. Additionally, this Passcode enables you to unlock your Smartcard if it becomes accidentally locked. The Account Recovery Passcode must be 8-20 characters in length, preferably alphanumeric and a mixture of upper/lower case.

- **Verification Passcode** is used to verify the identity of a user using a telephone service such as the NHS CRS Choose and Book application. The Verification Passcode must be 8-20 characters in length, preferably alphanumeric and a mixture of upper/lower case.

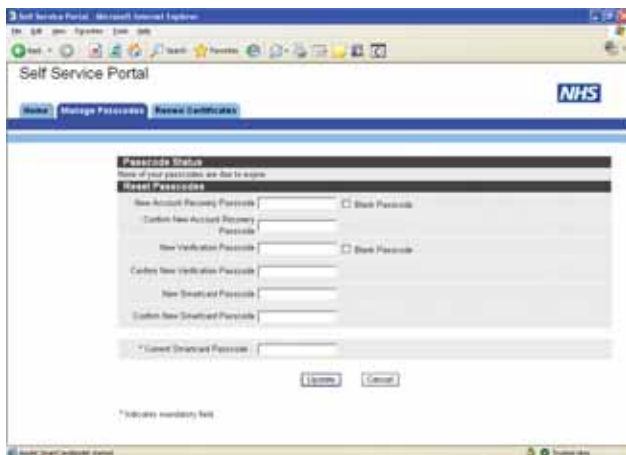
1.1 Passcode reset notification

You are automatically reminded to renew your Passcodes every 365 days. In the 14 days prior to expiry you will receive an alert once per day, and you can choose to renew your Passcodes at that time or decline and renew later. To renew upon receiving a notification, go to step 3 of the **How to set your Passcodes** procedure below.

If your Passcodes are not renewed within the 14 day notification period, you will be forced to renew at the next logon. If after a further 21 days you have not authenticated and changed your Passcodes, your account will be locked and you must visit the Registration Authority in your organisation to unlock it.

1.2 How to set your Passcodes

1. Authenticate to the NHS Spine
<https://portal.national.ncrs.nhs.uk/portal>.
2. Click **Launch Self Service Portal**.
3. From the Self Service Portal, click the **Manage Passcodes** tab.



The screenshot shows a web browser window titled 'Self Service Portal - Microsoft Internet Explorer'. The page is the 'Self Service Portal' with a navigation bar containing 'Home', 'Manage Passcodes', and 'Revoke Certificates'. The main content area is titled 'Passcode Status' and 'Reset Passcodes'. It contains several input fields for 'New Account Recovery Passcode', 'Current New Account Recovery Passcode', 'New Verification Passcode', 'Current New Verification Passcode', 'New Smartcard Passcode', and 'Current New Smartcard Passcode'. There are also checkboxes for 'Blank Passcode' for both Account Recovery and Verification. A 'Current Smartcard Passcode' field is at the bottom. 'Update' and 'Cancel' buttons are at the bottom right. A note at the bottom left states '* Indicates mandatory field'.

4. In **Reset Passcodes**, enter and confirm new Passcodes against those that you require, for example:
Account Recovery Passcode (8-20 characters)
Verification Passcode (8-20 characters)
Smartcard Passcode (4-8 characters)
Important: Any Passcode used in the last five Passcode changes will not be accepted, and you are strongly advised to synchronise and set all Passcodes you require at the same time.
5. If you choose to no longer have an Account Recovery Passcode or Verification Passcode after having one previously set, select the **Blank Passcode** box to remove pre-existing Passcodes.
6. Enter your existing Smartcard Passcode in the **Current Smartcard Passcode** box.
7. Click **Update**.
A message confirms your Passcodes have been updated successfully.

2 Certificate renewal notification

You are automatically reminded to renew your Smartcard certificates when they are close to expiry. You can renew your certificates twice without visiting your Registration Authority, at the third renewal you must visit your Registration Authority who will verify your identity and renew your certificates.

In the 30 days prior to certificate expiry you will receive an alert once per day. Upon receiving this message you can choose to renew your certificates at that time or decline and renew later. When certificates are within 20 days of expiry, you will be forced to renew.

2.1 How to renew your Smartcard certificates

1. At the renewal prompt click **Yes**. You are taken to the Self Service Portal.
2. Click the **Renew Certificates** tab. You are presented with **Update My Card** workflow.
3. Enter your Smartcard Passcode, to confirm your identity and the first certificate update.
4. Click **OK**.
Creating Card and Writing Certificates warnings appear one after another. A message indicates that the certificates have been renewed and the Smartcard has been updated successfully.
5. Click **Continue** to confirm the update.
6. Close the browser and authenticate again as normal.