1 Overview: Card Management Services – Smartcard Expiry Guidance (November 2017)

NHS Digital will be making an update to CMS (Card Management Services) within the CIS (Care Identity Service) application, to enable users to *self-renew* their Oberthur (Series 8) Smartcards. *Self-renew* is already available for users of Gemalto Smartcards – the CMS 2.2 release will make it available for all smartcards.

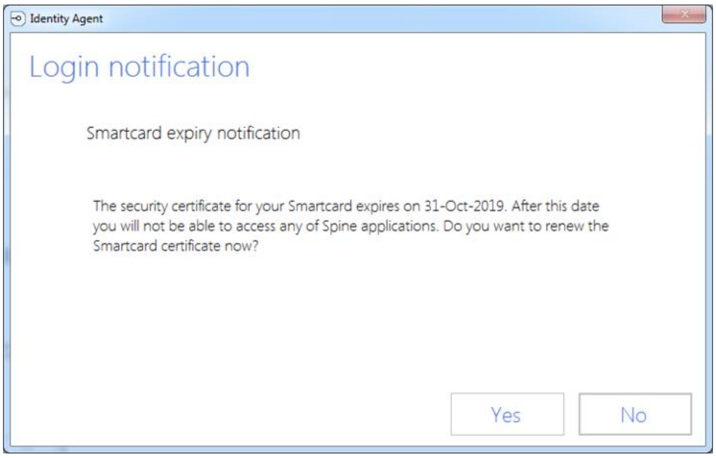
This RA (Registration Authority) and Smartcard User Guidance has been issued to support the implementation of CMS 2.2.

2 Why is self-renew being introduced for all smartcards?

- CMS 2.2 will enable users to self-renew their Series 8 Smartcards at their desk / workstation, without the need to install Oberthur Middleware, and without the need to visit their local RA.
- Prior to this release, Series 8 (Oberthur) Smartcards could be renewed but only if Oberthur Middleware was installed on the machine. However, whilst the RA community are required to install Oberthur Middleware in order to perform CMS operations on Series 8 Smartcards, for many reasons we want to avoid the whole of the NHS estate needing to install this additional middleware. The changes introduced in CMS 2.2 will remove the need for users to install Oberthur Middleware.
- The RA community will continue to be required to use Oberthur Middleware for all other CMS operations.

3 Smartcard expiry notifications

When a smartcard is approaching its expiry date, users will receive an expiry notification each time they log into Spine services using their smartcard. An example notification is shown below:



The security certificate for your Smartcard expires on 31-Oct-2019. After this date you will not be able to access any of Spine applications. Do you want to renew the Smartcard certificate now?

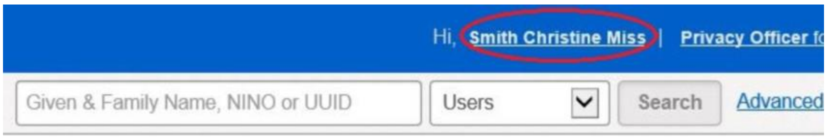
If users choose ‘Yes’, at this point they are directed to the CIS application – they are then able to follow the self-renew process for their smartcard (see Section 4 for more details). Alternatively, users may contact their local RA (Registration Authority) and request that they perform a smartcard renewal on their behalf.

If users answer ‘No’ they will still successfully authenticate, and no further action will be taken. However, if the smartcard is not renewed by the stated expiry date:

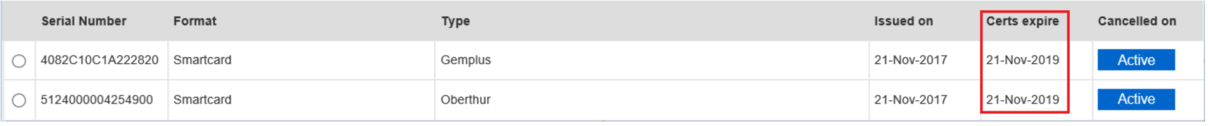
a) They will no longer be able to authenticate
b) Users will need to take their smartcard to their local RA and request an ‘RA-renewal’.

Users can find out their smartcard expiry date, either through the information provided on the ‘Smartcard expiry notification’ form (shown above), or by visiting their user profile page in CIS (Care Identity Service):

- User logs into CIS
- User clicks on their name at the top of the screen:


Hi, Smith Christine Miss | Privacy Officer fo
Given & Family Name, NINO or UUID
Users
Search
Advanced

- The user profile page will show all smartcards associated with the user’s Spine account. In the vast majority of cases, there should be just one smartcard shown.
- The smartcard expiry date is shown under the column ‘Certs expire’



	Serial Number	Format	Type	Issued on	Certs expire	Cancelled on
○	4082C10C1A222820	Smartcard	Gemplus	21-Nov-2017	21-Nov-2019	Active
○	5124000004254900	Smartcard	Oberthur	21-Nov-2017	21-Nov-2019	Active

4 Self-renew process

4.1 Step 1: knowing your smartcard type and identity agent version

There are currently two types of smartcard in use by Health and Care professionals within England:

- Gemalto Smartcards (a.k.a. Series 4, 5, 6)
- Oberthur Smartcards (a.k.a. Series 8)

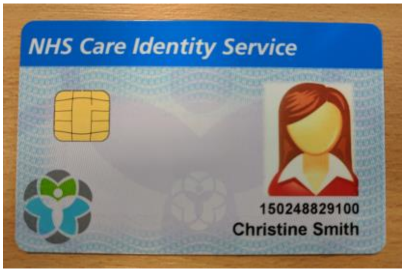
The process to self-renew varies slightly depending on the type of smartcard and IA (identity agent) version they use. Before undertaking a smartcard self-renew, users are advised to establish this information.

Once this is known, users should follow the relevant guidance below.

4.1.1 Identifying your smartcard type

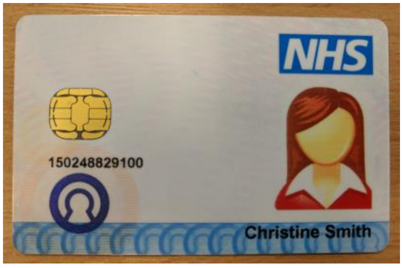
- **Series 8 Smartcards** display the header ‘NHS Care Identity Service’, and feature the CIS logo on the bottom-left of the smartcard. Below is an example of a Series 8 Smartcard. If this is your type of smartcard, please refer to the: Series 8 Smartcard – Self Renew Guidance section below.

Oberthur (Series 8) Smartcard

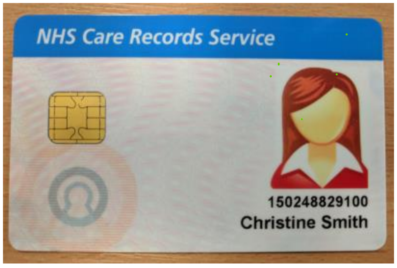


- **Gemalto (Series 4, 5, 6) Smartcards** display either no header, or 'NHS Care Records Service', and they do not have the CIS logo anywhere on the cards. Below is an example of a Gemalto Smartcard. If this is your type of smartcard, please refer to the Gemalto Smartcard – Self Renew Guidance section below.

Gemalto (Series 4) Smartcard



Gemalto (Series 5 or 6) Smartcard



Note: It is not necessary for users to identify their IA version in order to self-renew Gemalto Smartcards. In these cases, please go directly to the 'Gemalto Smartcards – Self-Renew Guidance' section below.

4.1.2 Identifying your identity agent version

There are five versions of IA (Identity Agent) that are supported for the purposes of Series 8 Smartcard self-renewal:

- BT IA v11
- BT IA v13
- NHS Digital IA v1.0 (previously HSCIC IA v1)
- NHS Digital IA v2.0 (previously HSCIC IA v2.0)
- NHS Digital IA v2.1.2.16

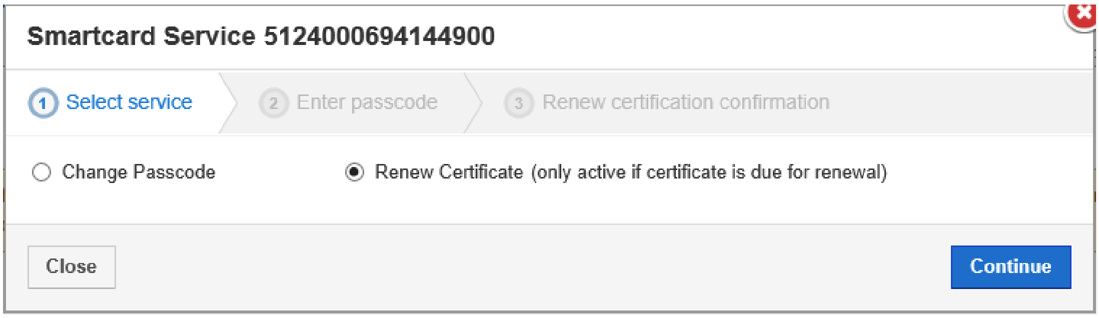
Other versions of IA will be actively blocked from completing a Series 8 Smartcard self-renewal, due to the likely resultant corruption of the smartcard. If you are unsure how to check your IA version, please contact your local RA / IT support team.

4.2 Step 2: Gemalto Smartcard – self-renew guidance

If during authentication with a Gemalto Smartcard, the user receives the 'Smartcard Expiry Notification' (see Section 3), the user should follow these steps:

1) Answer 'Yes' to the presented dialogue box, which logs them into the CIS application.

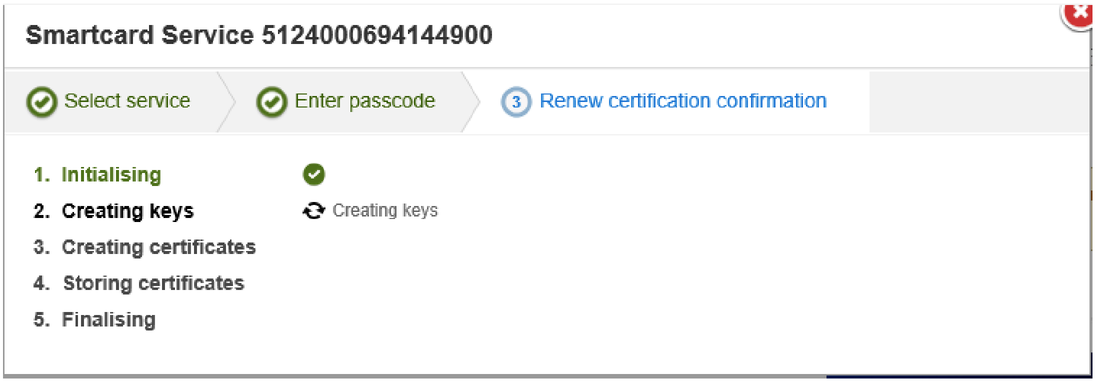
2) If the user has a single role, they will immediately be presented with the CMS form. Proceed to **Step 4**.
3) If the user has multiple roles, they will be sent to their 'User Profile' screen. From here the user can click on the 'radio button' for the relevant smartcard (based on the expiry date shown), and then click 'Service'. They will then be presented with the CMS form.
4) Click on the 'Renew Certificate' radio button, and click 'Continue'.



Smartcard Service 5124000694144900

○ Change Passcode ● Renew Certificate (only active if certificate is due for renewal)

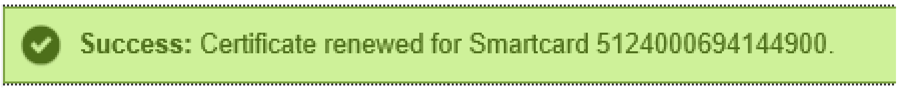
5) The application will now renew the security certificates held on your smartcard. This process should take around 1-2 minutes.



Smartcard Service 5124000694144900

1. Initialising ✓
2. Creating keys — Creating keys
3. Creating certificates
4. Storing certificates
5. Finalising

6) On completion of the self-renewal process, the CIS application should show something similar to the following message:



Success: Certificate renewed for Smartcard 5124000694144900.

7) The smartcard is now renewed, and valid for the next two years.

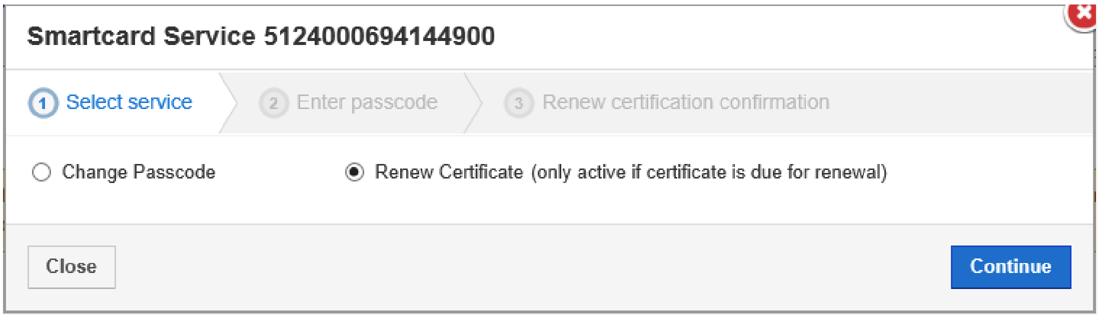
Note: depending on the IA in use, the user may get logged out of CIS at this point or shortly after – this is due to inbuilt security checks detecting a change in the smartcard. If this happens, simply log back in.

4.3 Step 2: Series 8 Smartcard – self-renew guidance

If during authentication with a Series 8 Smartcard, the user receives the 'Smartcard Expiry Notification' (see Section 3), the user should follow these steps:

1) Answer 'Yes' to the presented dialogue box, which logs them into the CIS application.
2) If the user has a single role, they will immediately be presented with the CMS form. Proceed to **Step 4**.

3) If the user has multiple roles, they will be sent to their 'User Profile' screen. From here the user can click on the 'radio button' for the relevant smartcard (based on the expiry date shown), and then click 'Service'. They will then be presented with the CMS form.
4) Click on the 'Renew Certificate' radio button, and click 'Continue'.

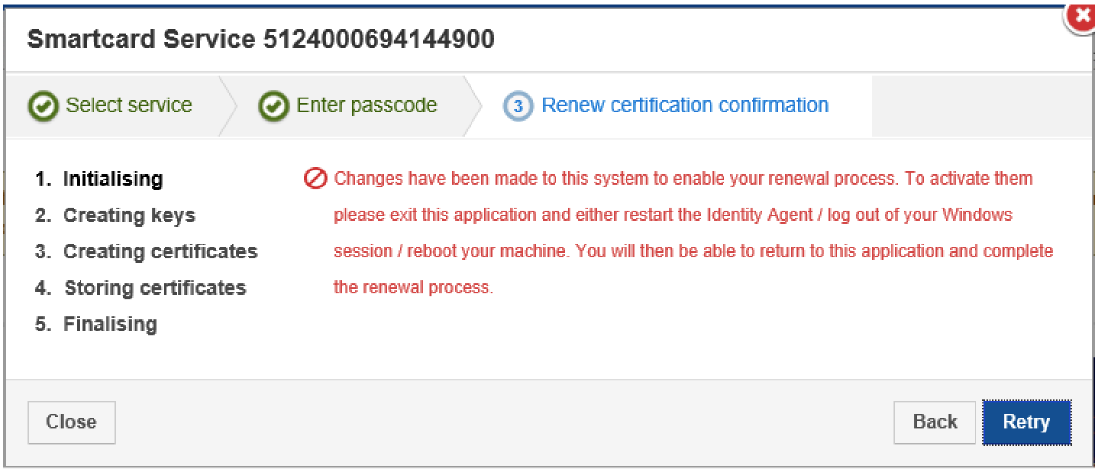


Smartcard Service 5124000694144900

1 Select service | 2 Enter passcode | 3 Renew certification confirmation

○ Change Passcode ● Renew Certificate (only active if certificate is due for renewal)

5) At this point, if using BT Identity Agents v11 or v13, proceed to **Step 6**. If using Identity Agents IA v1 or IA v2 it is likely the following message will be received:



Smartcard Service 5124000694144900

✓ Select service | ✓ Enter passcode | 3 Renew certification confirmation

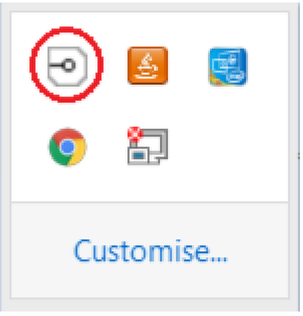
1. Initialising
2. Creating keys
3. Creating certificates
4. Storing certificates
5. Finalising

⊘ Changes have been made to this system to enable your renewal process. To activate them please exit this application and either restart the Identity Agent / log out of your Windows session / reboot your machine. You will then be able to return to this application and complete the renewal process.

Simply follow the advice. If you require more detail:

After logging out of the application (CIS), there are three possible options. They are presented in order of speed, however if you are unsure how to proceed the simplest option is to reboot your machine.

a) Restart the identity agent. Find the IA icon in your System Tray:



Right-click the icon, and choose 'Exit'. To start the identity agent again:

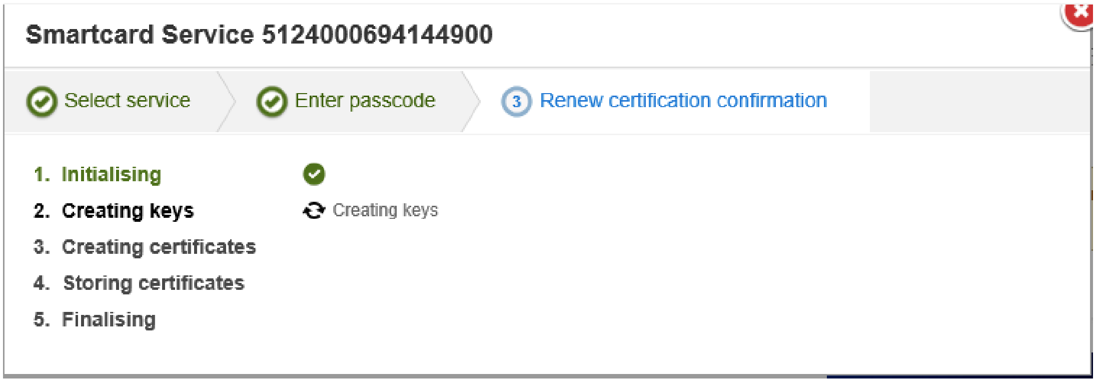
- **Windows 7:** Start / All Programs / Identity Agent/ Identity Agent
- **Windows 8.1 / 10:** Click on the Windows icon, search, 'Identity Agent'

b) Log out of your Windows session. Click on the Windows icon, select your Windows user icon, and log off / sign out of your Windows session. Log back into Windows.

c) Reboot your machine. Simply restart your machine – this is the simplest method however depending on the speed of your machine this process may take several minutes.

After following one of the above options, log back into the CIS application and start the renewal process again. This time, you should not receive the 'Changes have been made' message and self-renewal should proceed.

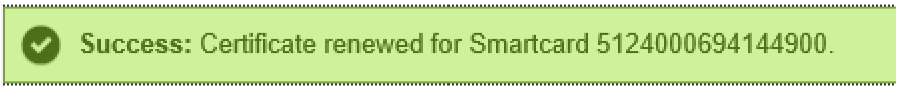
6) The application will now renew the security certificates held on your smartcard. This process should take around 1 minute if the user does not have Oberthur Middleware installed, and 2-3 minutes if they do.



Smartcard Service 5124000694144900

1. Initialising ✓
2. Creating keys — Creating keys
3. Creating certificates
4. Storing certificates
5. Finalising

7) On completion of the self-renewal process, the CIS application should show something similar to the following message:



Success: Certificate renewed for Smartcard 5124000694144900.

8) The smartcard is now renewed, and valid for the next two years.

Note: depending on the IA in use, the user may get logged out of CIS at this point or shortly after – this is due to inbuilt security checks detecting a change in the smartcard. If this happens to you, simply log back in.

5 Support

Additional guidance has been provided should users experience problems either during the self-renewal process, or any subsequent authentication attempts.

Note: If issues persist, please contact your local RA, or log a call with the National Service Desk on https://nww.nhscfhservicedesk.nhs.uk/NSD/servlet/NSDLogin or 0300 30 35 035

5.1 Problems encountered during self-renewal

5.1.1 "Changes have been made to this system to enable your renewal process..."

This message is received if the user is attempting a self-renewal of a Series 8 Smartcard, whilst using any version of IA v1 or IA v2.

Simply follow the instructions given. For more detail refer to Section 4.3 'Series 8 Smartcard – self-renew guidance'.

5.1.2 "There was a problem deleting your key container" or "Failed to create keys"

This message may be received if the Series 8 Smartcard has become corrupted since it was originally issued – despite the fact the user may have had no previous problems authenticating with it (the renewal process makes additional smartcard integrity checks).

The user can make another attempt by clicking on 'Retry', but in these cases often the only practical course of action is for the user to request that their local RA cancels this smartcard, and re-issues it. If further problems are experienced, issuing a completely new smartcard may be necessary.

5.1.3 "Series 8 Smartcard renewal is not currently supported on this machine. The installed identity agent is not compatible"

The most likely cause of this error is that the identity agent in use is not supported for Series 8 Smartcard self-renewal (see section 'Identifying your identity agent version').

If the user's identity agent is supported, this error can occur if the user's machine has a) been strictly 'locked down' by its administrators, or b) has an alternate 'Admin' Windows account which prevents full access to the registry. The Series 8 Smartcard self-renewal process requires read-only access to the user's full registry, and write access to the 'HKEY_CURRENT_USER' area. If this is prevented, the renewal process cannot detect your identity agent type, and the above error will be received.

In these cases, the user should either seek to perform the smartcard self-renewal on a machine with more 'relaxed' security settings, or ask that their administrator alters the security settings on their own machine, such that the above registry permissions are allowed.

5.1.4 User gets logged out after successful self-renewal

Once a smartcard has been renewed the security certificates on it have been altered. Due to checks periodically performed by all versions of Identity Agent, the smartcard may be therefore be deemed different to that which originally authenticated – with the result that the IA logs the user out.

If this happens, simply log back in – the error should not reoccur.

5.2 Problems encountered during authentication

5.2.1 "There was a problem reading your smartcard" or "Your smartcard is empty"

The smartcard has been placed into a state unrecognisable by the identity agent, either by the self-renew process, or by a previous CMS operation on that smartcard, causing an issue that has lain 'dormant' but exposed by self-renewal.

There are a couple of potential workarounds. It should be noted that the 'Gem Heal' fixes are only possible on machines that have Gemalto Middleware only (not Oberthur).

5.2.1.1 Perform a 'Gem Heal' via Classic Client Toolbox

Note: Classic Client Toolbox should only be used to perform the following operation, and only when encountering this particular issue. Use of this tool on a smartcard in any other state may render it unusable.

1) Put the smartcard into a Gemalto middleware-only machine
2) Launch 'Classic Client Toolbox' from Windows (this is a Gemalto middleware admin app that gets installed by default when Gemalto middleware is installed - it is possible that local Deployment teams may have blocked it)
3) Click on <Card Properties>
4) Select the appropriate smartcard reader, and click <Next>
5) Enter the smartcard's passcode in the 'PIN Code' field, and click <Login>
6) Click <Advance>, and then <Diagnosis>
7) User should receive the message 'Operation complete'
8) Attempt to authenticate with smartcard

5.2.1.2 Perform a 'Gem Heal' via BT Identity Agent v13

1) Authenticate with BT Identity Agent v13 in a Gemalto middleware-only machine (this is likely to mean using a machine other than the user's original machine, as this kind of issue typically occurs with IA v1 or IA v2)
2) If the user is able to authenticate successfully, they should receive the message 'Updating your smartcard…'
3) After a few seconds the user should receive the message 'Your smartcard has been updated'
4) Attempt to authenticate in the original machine the problem was experienced on

5.2.1.3 Smartcard cancel / re-issue

If neither of the above fixes are workable, the only practical course of action is for the user to request that their local RA cancels this smartcard, and re-issues it (an RA smartcard repair will not work in this instance). If further problems are experienced, issuing a completely new smartcard may be necessary.

5.2.2 'The security certificate for your Smartcard expires on *<date>'* or 'Your Smartcard has expired'

These errors can occur if the user has self-renewed their Series 8 Smartcard on a machine that *only* has Gemalto Middleware installed, and then subsequently attempted authentication on a machine that *also* has Oberthur middleware installed.

In these cases, the user should either revert to a machine that only has Gemalto Middleware, or ask their RA to cancel / re-issue their smartcard.

6 Specific guidance to Registration Authorities

6.1 Background

As we know, security certificates on smartcards expire two years after issuance. Since the very first Series 8 Smartcards were issued in the Live environment mid-November 2015, Series 8 Smartcards started to expire from mid-November 2017. Series 8 Smartcards continue to expire in increasing amounts, peaking at approx. 800 expiries a day in early March, and falling back to an average of around 400-700 expiries per day.

As explained in Section 2, whilst Gemalto Smartcards continue to be self-renewable by all smartcard holders due to the installation of Gemalto middleware across the whole estate, Series 8 Smartcards could only previously be renewed on machines where Oberthur middleware was installed.

As a result of the CMS 2.2 release, all users can now self-renew Series 8 Smartcards, through the use of a series of .DLL files that are downloaded to the users' machines during the self-renewal process.

6.2 User experience

The self-renewal process for Series 8 Smartcards is intended to be identical to that of Gemalto Smartcards. The only noticeable difference will be the message received and subsequent action required when IA v1 or IA v2 is used for the process. This is detailed in 'Section 4.3 – Series 8 Smartcard – self-renewal guidance'.

However, it is possible that some users may be nervous about starting this process, or if they receive the message about system changes, and this may result in a call to their local RA.

It is unlikely, but also possible, that users may experience technical difficulties during or immediately after this process.

6.3 Possible actions

6.3.1 Additional user guidance

In the cases where users require guidance / reassurance, we advise the RA talks the user through the process.

Of course, it is also possible for the RA to perform an 'RA-renewal' of the user's Series 8 smartcard (assuming the RA has installed Oberthur middleware), instead of the user performing self-renewal. However, since RA-renewal requires the presence of both the smartcard and its holder, this may not be convenient.

As a last resort, the RA may issue a fresh Series 8 Smartcard, and follow the normal process for sending this to the user. In these cases, the original smartcard should be remotely cancelled by the RA (despite the fact the original smartcard will soon expire if it is not renewed anyway).

6.3.2 Problems experienced by user

Should users experience problems with Series 8 Smartcard self-renewal, they are advised to work through 'Section 5 – Support'.

Again, depending on the circumstances of the user, the RA may choose to issue a fresh Series 8 Smartcard, and follow the normal process for sending this to the user. In these cases, the original smartcard should be remotely cancelled by the RA (regardless of the state the original smartcard is left in).