

Registration Authorities: Arrangements for Temporary access to NHS CRS applications

30th September 2008

Registration Authorities: Arrangements for Temporary access to NHS CRS applications

30th September 2008

30th September 2008

Contents

1	Overview	3
1.1	Purpose and Audience	3
1.2	Background.....	3
1.3	Policy Considerations	4
1.4	Self Service Fallback Smartcard	5
1.5	Self Service Fallback Smartcard creation	5
1.6	Self Service Fallback Smartcard use.....	6
1.7	Self Service Fallback Smartcard return	6
1.8	Short-term Access Smartcard	6
1.9	Pre-populated Short-term Access Smartcard creation.....	7
1.10	Pre-populated Short-term Access Smartcard use	7
1.11	Pre-populated Short-term Access Smartcard return	7
2	Detailed Guidance on Self Service Fallback.....	8
2.1	Responsibilities for Self Service Fallback Smartcards	8
2.2	Self Service Fallback Smartcard Creation.....	9
2.3	Issuing and Monitoring Usage of Fallback Smartcards	9
2.4	Process for Assigning Self Service Fallback Smartcards to Users	10
2.5	End of Usage Period	11
2.6	Process for the Return of Self Service Fallback Smartcards	11
3	Detailed Guidance on Pre-populated Short-term Access Smartcards	11
3.1	Responsibilities for pre-populated Short-term Access Smartcard solution	11
3.2	Short-term Access Smartcard Creation.....	12
3.3	Standard Short-term Access Smartcard image.....	13
3.4	Issuing and Monitoring Usage	13
3.5	Audit.....	13
3.6	Process for Assigning Short-term Access Smartcards.....	14
3.7	End of Usage Period	15
3.8	Process for the Return of Short-term Access Smartcards	15
4	Appendices	16
4.1	Appendix A – RA04	16
4.2	Appendix B – RA09	17

30th September 2008

1 Overview

1.1 Purpose and Audience

This document is written to provide consolidated guidance on the production, issuance, and use of Self Service Fallback and Short-term Access Smartcards.

This document has been written for Registration Authority managers, Registration Authority agents, sponsors, HR/Medical Staffing managers and those responsible for Information Governance arrangement in the NHS organisations who are going to be involved in the provision of temporary access to users of NHS CRS applications where the individual does not:

- a) have access to their own Smartcard because it has been forgotten, lost, stolen or broken in which case a Self Service Fallback Smartcard is used; or
- b) where an NHS CRS Smartcard holder cannot get an appropriate access profile for the organisation, location, or role they will be undertaking because there is no Registration Authority available (e.g. temporary/locum and agency staff arriving out of office hours) in which case a pre-populated Short-term Access Smartcard is issued.

It is a requirement of access to the NHS CRS that users have an NHS CRS Smartcard, issued by an NHS organisation's Registration Authority (RA). Under current policy it is not possible for temporary staffing agencies (TSAs) to have their own RA and therefore the governance responsibility for those staff provided by TSAs stays firmly within the NHS and sits alongside the responsibility for patient safety and confidentiality. This means that local NHS organisations will have to consider options for the provision of Smartcards for temporary/locum staff, alongside the provision of NHS CRS Smartcards for their own employed staff.

This paper does not address the mechanism by which local organisations will seek to initially register those staff provided by TSAs. However it is critical that the provision of NHS CRS Smartcards to those workers, who provide NHS care and who need access to the NHS CRS, is managed effectively.

This demands close working between temporary staffing agencies and NHS organisations (particularly RA, HR, and medical staffing departments) over the identification of individuals who will need to be registered for an NHS CRS Smartcard. It will also require RAs to understand the local processes, key staff, and the metrics surrounding the usage of temporary/locum staff. Any solution must involve the audience above.

1.2 Background

NHS CRS applications and applications that use the NHS CRS Spine for authentication require users to authenticate with a Smartcard and Passcode. It is recognised that on occasions the Smartcard may not be available to the individual because of one of the following reasons:

- The individual's Smartcard has been forgotten, lost, stolen, or broken
- The individual may need to provide services in a location or role for which they do not have an appropriate access profile either because they are providing the service at a new location or the activities are not appropriate for the role being undertaken either on a permanent or temporary basis.

It is envisaged that with the introduction of the software upgrade in 2009, the vast majority of the latter causes will be managed by Position Based Access Control.

This paper assumes that all staff needing temporary access to NHS CRS, whether permanent or temporary/locum staff, have an NHS CRS Smartcard and have therefore had their identity checked to e-GIF Level 3 by an NHS organisation's RA for the purpose of access control.

This paper should be read in conjunction with "Guidance on the Registration of temporary staff working within the NHS" - NPFIT-SI-SIGOV-0041.01, and "Registration Authorities Operational Process and Guidance" v2.0 (or later) - NPFIT-FNT-IMD-IME-0182.10.

30th September 2008

1.3 Policy Considerations

There are several important policy considerations in relation to the issuance of Self Service Fallback Smartcards and Short-term Access Smartcards:

Does the individual need access to the NHS CRS application for the duration of their shift?

The nature of the activities being undertaken may not require access to the application or the interactions can be done on the individuals behalf by another e.g. look up blood results.

The overriding factor is whether there is risk to healthcare provision or significant business impact.

Does the individual already have a Smartcard?

Self Service Fallback Smartcards and Short-term Access Smartcards can only be issued to individuals who have been approved by a sponsor as needing a Smartcard, have proved their identity beyond reasonable doubt (e-GIF Level 3), **and** have evidence of this via an NHS CRS Smartcard bearing a true likeness photograph.

Where the individual has forgotten or lost their Smartcard it is essential that the identity is confirmed by face-to-face comparison with the individual's photograph as recorded on the Card Management System.

'Partial Registrations' e.g. just a record on the Spine User Directory are unacceptable as this could lead to multiple open profiles due to multiple registrations.

Can another process other than use of a Self Service Fallback Smartcard or Short-term Access Smartcard be utilised to support the individual's provision of healthcare?

It should be possible during the working hours of the Registration Authority to re-issue the Smartcard where a Smartcard has been lost or stolen.

Where an individual may need to provide services in a location or role for which they do not have an appropriate access profile either because they are providing the service at a new location or the activities are not appropriate for the role being undertaken either on a permanent or temporary basis then the following two options should be considered in the first instance:

Option A – Using the UUID to add the profile in advance of the shift

This applies where the location/role change or temporary/locum member of staff is planned in advance and the identity of the individual is known including the UUID. It can apply whether the individual is booked to arrive either inside or out of office working hours.

The RA02 would then be completed either by the line manager making the change or the person who books the temporary member of staff and signed by a sponsor. Where the individual does not have a Smartcard then arrangements must be put in place to obtain a Smartcard prior to them starting work.

Option B – Profile granted at commencement of shift

This applies where the location/role change or temporary/locum member of staff is arranged at short notice, the identity is unknown and they arrive when RA staff are available.

If they cannot complete Option A above, they should arrange for the individual to arrive in enough time to enable the profile to be granted at the commencement of their shift. On arrival the RA should confirm the individuals NHS CRS Smartcard. The sponsor for the access rights should complete and sign the RA02 and the RA agent should grant the rights prior to the commencement of the shift in accordance with the standard RA process (refer to *"Registration Authorities Operational Process and Guidance" v2.0 - NPFIT-SI-SIPROJ-0533*).

Where an organisation is using Position Based Access Control, and an appropriate position has been sponsored and the position to be undertaken by the individual is evidenced the RA agent can grant the pre-approved access rights without the further requirements of sponsorship.

These options should always be considered prior to the use of a Short-term Access Smartcard.

30th September 2008

Is the organisation assured that the individual is adequately trained and understands their obligations to the NHS Code of Confidentiality and Care Record Guarantee prior to the issuance of the Fallback Smartcard?

It is a matter for the local organisation to decide what training is required prior to the individual starting their shift.

Where these policy considerations have been made and it is felt that a Self Service Fallback Smartcard or a Short-term Access Smartcard is an appropriate method of access for the NHS CRS application then the organisation has the following two possible methods of providing temporary access to NHS CRS applications:

- **Use of Self Service Fallback Smartcard**

This is appropriate where the user has an access profile relating to the role they need to undertake e.g. where the user's Smartcard has been forgotten, lost, stolen, or broken.

- **Use of pre-populated Short-term Access Smartcard**

This is appropriate when the user does not have a profile relating to the role they need to undertake e.g. staff working in another location or role within the organisation or temporary staff, or

Where Self Service Fallback Smartcards are unobtainable due to the availability of a custodian at the location, or when the user does not have an @nhs.net email account or mobile phone number recorded in the Spine User Directory.

1.4 Self Service Fallback Smartcard

The 2008A Spine release enables a user who forgets or loses their Smartcard to associate their current user role profile with a blank Fallback Smartcard. This functionality has several governance advantages:

- The UUID recorded as having accessed the NHS CRS application will be traceable to the individual without the need to reference a RA04.
- The access profile will be appropriate to the user's role as it will be the same so there is no risk of the need to issue a 'best fit' Short term access Smartcard therefore improving patient safety and confidentiality.
- Where the user has lost their Smartcard the functionality will automatically cancel the original Smartcard so preventing improper use if found by someone other than the user.
- Where the user has forgotten their Smartcard the functionality will suspend the original Smartcard for the duration of the Self Service Fallback issuance or 12 hours, whichever is longer.

Below is a summary of the process. Detailed guidance can be found in section 2 "*Detailed Guidance on Self Service Fallback*".

1.5 Self Service Fallback Smartcard creation

RA managers and RA agents can create Fallback Smartcards and associate them with a custodian. A custodian will need to be a clinician/manager who has responsibility for a particular clinical or administrative area, they need not be a sponsor. The custodian will need to develop a process for managing the use of Fallback Smartcards out of normal office hours if necessary.

To create a Self Service Fallback Smartcard:

- A sponsor within the organisation requests a Self Service Fallback Smartcard via an RA09 (refer to section 4.2 Appendix B – RA09)
- From the Registration screen, the RA selects **Fallback Accounts** and **Create** and associates it with a custodian (a registered user) using the **Custodian** field
- The naming convention in the **Name** field should be Organisation code FBS 1, where '1' is one of a number of Fallback Smartcards associated with the custodian
- The Fallback Smartcard is printed (see example below)

30th September 2008



1.6 Self Service Fallback Smartcard use

To assign a Self Service Fallback Smartcard:

- User obtains a Self Service Fallback Smartcard from a custodian and navigates to the Smartcard Service Centre, <http://portal.national.ncrs.nhs.uk/scsc>.
- User inserts the Self Service Fallback Smartcard into the card reader and the system recognises that the Smartcard is a Fallback Smartcard.
- System prompts the user for their name, UUID, and Account Recovery Passcode.
- User receives a system generated one time Passcode via a secure channel (SMS text message or email to an @nhs.net email account). **Note:** The one time Passcode must be used within 10 minutes of it being requested, it will not be valid after this.
- User enters the one time Passcode and the system assigns the Fallback Smartcard to the user. System requests reason for use of the Fallback Smartcard:
 - Smartcard lost or stolen or broken
 - Smartcard forgotten

In the first case the users Smartcard will be revoked and in the second the Smartcard will be suspended while the user is using the Fallback Smartcard.

- User sets the Passcode to be associated with this use of the Fallback Smartcard. When set the user can log on for up to 12 hours with the Self Service Fallback Smartcard as though it were their own.

The Self Service Fallback Smartcards when used by a user inherit the users UUID and access profile(s), including those for other organisations they have profiles for.

Fallback Smartcards do not have the use of the user's content commitment certificate. If the user needs to digitally sign as part of their normal work process they will be unable to do this.

1.7 Self Service Fallback Smartcard return

To un-assign and return a Fallback Smartcard:

- User navigates to the Smartcard Service Centre (SCSC) and inserts the Fallback Smartcard into the card reader.
- System recognises the Fallback Smartcard is assigned to a user (expired or not) and removes the assignment and locks the Fallback Smartcard ready for its next assignment.
- User gives the Smartcard back to the custodian.

If a user does not return the Smartcard after the 12 hour period, the associated access will be removed and the Fallback Smartcard will cease to work. When it is returned and the assignment removed via the SCSC, it may be reused.

1.8 Short-term Access Smartcard

If the Self Service Fallback Smartcard is not appropriate, for reasons already stated, the RA manager should ensure that Options A and B described in section 1.3 "*Policy Considerations*" become good practice within their organisation and that Option C below Provision of a profile via a Short-term Access Smartcard is the exception rather than the rule.

Option C – Provision of profile via a Short-term Access Smartcard

30th September 2008

This applies where the location/role change or temporary/locum member of staff are arranged at short notice, or where their identity or UUID is unknown until they arrive, or they arrive when there are no RA staff available, or where approve and grant access rights cannot be given at that point in time.

This option can also be used where Self Service Fallback Smartcards are unavailable either due to availability of a custodian at the location or where the user does not have an @nhs.net email account or mobile phone number recorded in the Spine User Directory, or the user doesn't know his/her account recovery Passcode, or digital signing is required.

An organisation will need to consider which profiles are to be applied to Short-term access Smartcards, and in particular where workgroups are utilised, and which workgroups these Smartcards should be associated with.

Below is a summary of the process. Detailed guidance can be found in section 3 "*Detailed Guidance on Pre-populated Short-term Access Smartcards*".

1.9 Pre-populated Short-term Access Smartcard creation

The creation of a pre-populated Short-term Access Smartcard uses the same functionality as for a user's standard Smartcard.

To create a pre-populated Short-term Access Smartcard:

- A sponsor within the organisation requests a pre-populated Short-term Access Smartcard via an RA01.
- A standard profile is populated via an RA02
- From the Registration screen, the RA creates a Smartcard using the standard Smartcard creation process.
- The naming convention should be SAS – Sponsor Forename Sponsor Family Name – Profile Identifier e.g. A&E Nurse 1 [SAS – John Smith – A&E Nurse 1]
- The photo should be replaced with the image identified in section 3.3 "*Standard Short-term Access Smartcard image*".

1.10 Pre-populated Short-term Access Smartcard use

To obtain a pre-populated Short-term Access Smartcard:

- User meets with a sponsor who holds the SAS Smartcard.
- Sponsor assures themselves beyond reasonable doubt of the identity of the user either:
 - by checking the likeness against the Smartcard photo in the case of temporary/locum staff
 - by checking the users photo on CMS and checking that the card has not been revoked
 - by checking appropriate identity documents
- When assured of the identity the pre-populated Short-term Access Smartcard is unlocked and the user requested to set the Passcode for the session.
- Sponsor completes an RA04 (refer to section 4.1 Appendix A – RA04) recording the UUID and name of the Short-term Access Smartcard, UUID of the user, reason for issue, and start date and time.
- User must be made aware of the return time when they must return the Short-term Access Smartcard (sponsor to determine); this must be no more than 12 hours from the time of issue.
- Issuer completes the RA04 with the return time and sends to the RA.

1.11 Pre-populated Short-term Access Smartcard return

Smartcards should be returned to an appropriate sponsor by the user on or before the return time. (No greater than 12 hours from the time of issue.) The sponsor of the Smartcard should lock the Smartcard when it has been returned, by entering a random Passcode three times. If the Smartcard is not returned at or before the return time the issuer should notify the RA of the failure to return the Smartcard as soon as possible and complete an RA03. The RA will then remove the profile(s) and cancel the card associated with the Short-term Access Smartcard.

30th September 2008

If the Short-term Access Smartcard is reported lost, stolen, or damaged the RA will revoke the Short-term Access Smartcard certificates using an RA03.

Additionally, the RA04 should be completed to reflect the return time.

2 Detailed Guidance on Self Service Fallback

2.1 Responsibilities for Self Service Fallback Smartcards

Executive Management Team responsibilities

The organisation's Executive Management Team will ensure that:

- there is an organisation-based Self Service Fallback Smartcard process aligned with this procedure, which is operated by the local Registration Authority
- the organisation's support processes for Self Service Fallback Smartcards are documented within the local Registration Authority Operational Procedure manual.

Registration Authority responsibilities

The organisation's Registration Authority will:

- develop a Self Service Fallback Smartcard distribution and usage policy for the Executive Management Team (including audit policy). This will identify which individuals in the organisation will be custodians of Self Service Fallback Smartcard(s)
- note the profiles of RA manager, RA agent, and sponsor are not available with Fallback Smartcards
- communicate to users how the Self Service Fallback Smartcard process operates and what they need to know i.e. their Account Recovery Passcode and UUID.

RA manager's responsibilities

The RA manager will ensure:

- that all appropriate custodians defined by the Self Service Fallback Smartcard distribution and usage policy are trained in issuing and management of Self Service Fallback Smartcards
- users are aware of the claiming process and the need to know their Account Recovery Passcode and UUID, including how to update their Account Recovery Passcode and how to record their @nhs.net email account and/or mobile phone number in the Self Service Portal
- RA Reporting is used to confirm/monitor Self Service Fallback Smartcard usage.

RA agent responsibilities

The RA agent(s) will ensure:

- Self Service Fallback Smartcards are issued in accordance with national and local policies
- when not in use, that Self Service Fallback Smartcards are kept in a secure location
- appropriate individuals are supported in the usage of Self Service Fallback Smartcards in accordance with the Fallback process.

RA sponsor's responsibilities

The sponsor will ensure:

- that requests for Self Service Fallback Smartcards are requested via an RA09.

Custodians' responsibilities

The custodians identified in the Self Service Fallback Smartcard distribution and usage policy as nominated individuals in relation to the issuing of Fallback Smartcards will ensure:

- Self Service Fallback Smartcards are issued in accordance with the Fallback process

30th September 2008

- that certificates of a Self Service Fallback Smartcard when close to expiry are renewed by their local RA.

2.2 Self Service Fallback Smartcard Creation

The local RA will issue Self Service Fallback Smartcards only to individuals identified in the Self Service Fallback Smartcard distribution and usage policy as nominated officers.

These Smartcards will have RA09s (refer to section 4.2 Appendix B – RA09) completed for them as below:

Form field	Entry for single issuer administration
Custodian Name	Name of the custodian who is going to be responsible for the Fallback Smartcard
Custodian Smartcard UUID	Custodians UUID
Fallback Smartcard Name	The naming convention is Organisation code FBS 1
Fallback Smartcard UUID	The UUID of the Fallback Smartcard
Organisation	The NHS organisation that uniquely identifies the organisation in which the Fallback Smartcard will be used
Code	The NHS organisation code that represents the organisation in which the Fallback Smartcard will be used
Name (RA agent/manager)	Name of RA agent or manager
Smartcard UUID (RA agent/manager)	UUID of RA agent or manager
Date completed (RA agent/manager)	Date the RA agent or manager completes the form
Custodian's signature	Custodian must sign and date the form

2.3 Issuing and Monitoring Usage of Fallback Smartcards

It is recommended that the RA manager produces regular reports detailing:

- the number of Self Service Fallback Smartcards that have been issued
- who is the custodian of these Self Service Fallback Smartcards
- who has been using Self Service Fallback Smartcards and the extent of their usage
- the purpose of the usage i.e. lost Smartcards, forgotten Smartcards etc.

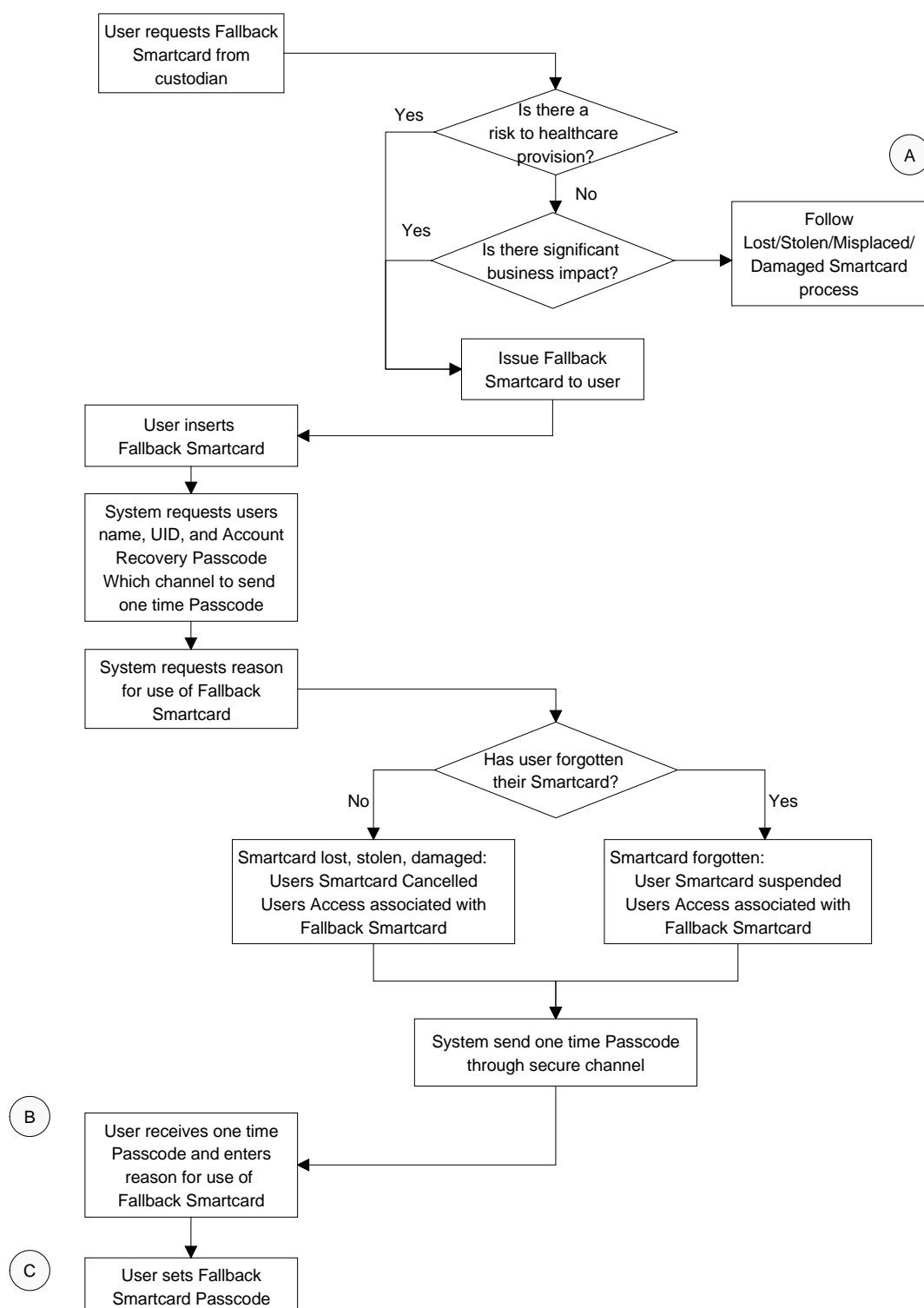
The RA manager then needs to satisfy themselves, that the usage has been appropriate and if not take appropriate remedial action.

Note: When Self Service Fallback Smartcard certificates are due to expire, there will be no automatic renewal notification. The custodian of the Self Service Fallback Smartcard should be aware of this and request a certificate renewal with their local RA at an appropriate time.

30th September 2008

2.4 Process for Assigning Self Service Fallback Smartcards to Users

The flowchart below illustrates the process issuers will follow when assigning a Self Service Fallback Smartcard to healthcare professionals/workers.



Notes	Description
A	Need to determine why the user hasn't got their Smartcard and follow appropriate course with user and possibly Lost/Stolen/Misplaced/Damaged Smartcard Process
B	User receives one time Passcode and confirms it back to the system within the ten minute validity period.
C	User has 12 hours use of the Smartcard before the claim period expires.

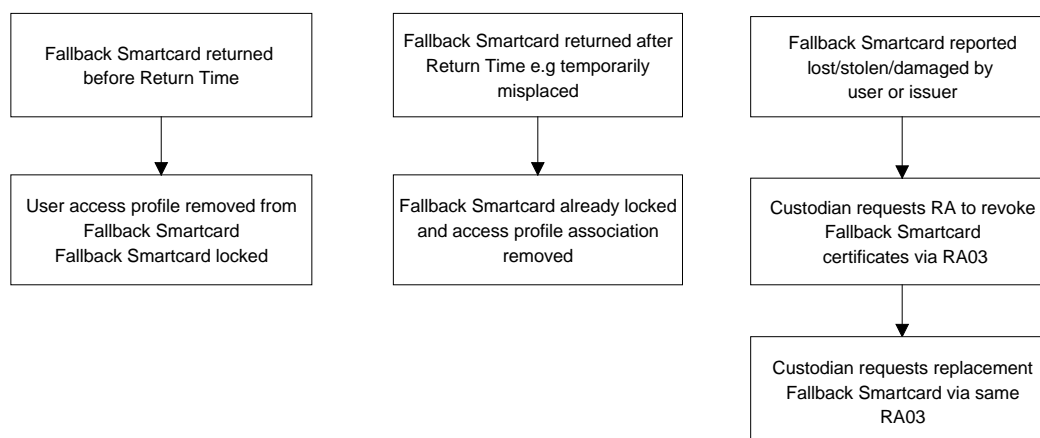
30th September 2008

2.5 End of Usage Period

If the Self Service Fallback Smartcard is not returned before 12 hours, the Self Service Fallback Smartcard will automatically lock itself.

If the Self Service Fallback Smartcard is reported lost, stolen, or damaged the RA will revoke the Self Service Fallback Smartcard.

2.6 Process for the Return of Self Service Fallback Smartcards



3 Detailed Guidance on Pre-populated Short-term Access Smartcards

3.1 Responsibilities for pre-populated Short-term Access Smartcard solution

Executive Management Team responsibilities

The organisation's Executive Management Team will ensure:

- there is an organisation based Short-term Access Smartcard process aligned with this procedure, which is operated by the local Registration Authority
- the organisation's support processes for Short-term Access Smartcards are documented within the local Registration Authority Operational Procedure manual.

Registration Authority responsibilities

The organisation's Registration Authority will:

- develop a Short-term Access Smartcard distribution and usage policy for the Executive Management Team (including audit policy). This will identify which individuals in the organisation should be able to distribute Short-term Access Smartcard(s) and what active (pre-loaded) profiles are associated with them. Note the profiles of RA manager, RA agent, and sponsor are not permitted
- communicate to users how the Short-term Access Smartcard process operates.

RA manager's responsibilities

The RA manager will ensure:

- that all appropriate individuals defined by the Short-term Access Smartcard distribution and usage policy are trained in issuing and managing Short-term Access Smartcards including the usage of the RA04
- users are aware of their responsibilities in using and returning the Short-term Access Smartcard.

RA agent responsibilities

30th September 2008

The RA agent(s) will ensure:

- Short-term Access Smartcards are issued in accordance with national and local policies
- when not in use, that Short-term Access Smartcards are kept in a secure location
- that all supporting RA04 forms are completed for the issue of Short-term Access Smartcards
- where notified by the Short-term Access Smartcard issuers that a Smartcard has exceeded the return time, the profiles associated with the Short-term Access Smartcard are revoked in a timely fashion
- appropriate individuals are supported in the usage of Short-term Access Smartcards in accordance with the Short-term Access process.

Sponsor responsibilities

Sponsors will ensure:

- Short-term Access Smartcards are issued in accordance with national and local policies
- where additional roles or activities are requested in relation to the Short-term Access Smartcards these are appropriate to the registered user requiring them
- they have seen the NHS CRS Smartcard associated with the temporary/locum staff and confirmed their identity
- they have unlocked the Short-term Access Smartcard at the beginning of the period of temporary usage and ensured that it is locked at the end of the period
- when not in use, that the Short-term Access Smartcards are kept in a secure location
- they have completed the details on the RA04 and sent it to the RA following the return of the Short-term Access Smartcard.

3.2 Short-term Access Smartcard Creation

The local RA will issue Short-term Access Smartcards only to individuals identified in the Short-term Access Smartcard distribution and usage policy as nominated officers.

These Smartcards will have RA01s completed for them; Part 1 will be completed by the RA as below:

Form field	Entry for single sponsor administration
First Name	First name of the sponsor who is going to be responsible for the Short-term Access Smartcard
Middle Name	Leave blank
Family Name	Family name of the sponsor who is going to be responsible for the Short-term Access Smartcard. This is preceded by 'SAS' where SAS allows 'easy' identification of the Short-term Access Smartcards, and followed by 'x'; where x is a sequential letter denoting that this is the 1 st , 2 nd or 3 rd . Short-term Access Smartcard issued to the sponsor e.g. SAS – John Smith – A&E Nurse 1, SAS – John Smith - A&E Nurse 2 etc.
Organisation Name	The NHS organisation code that uniquely identifies the organisation where the Short-term Access Smartcard will be used
Site Name	The NHS code which strongly links the organisation or site(s) where the Short-term Access Smartcard will be used
Telephone number	Issuer's desk phone or mobile number

Short-term Access Smartcards contain a typical profile for the work area in which it will be used. The use of pre-loaded profiles will be a local policy decision and the risk implications of doing this must be fully recognised.

A Smartcard will be loaded with a typical profile, and this should be detailed in an associated RA02 and signed by a sponsor and applied by the RA.

30th September 2008

The RA will then proceed to issue the Short-term Access Smartcard following the usual registration process, except that:

- instead of a photograph a standard Short-term Access Smartcard image will be used, refer to 3.3 “Standard Short-term Access Smartcard image” in the next section
- a random Passcode should be given to the Smartcard.

3.3 Standard Short-term Access Smartcard image



3.4 Issuing and Monitoring Usage

When a role/location change or temporary/locum member of staff is booked the sponsor will assess, in line with their local distribution policy, whether there is a real need for the use of a Short-term Access Smartcard i.e. there is a risk to the provision of healthcare or there is a significant business impact of not having access to NHS Care Records Service compliant applications.

For each issuance of a Short-term Access Smartcard, the sponsor should complete the RA04 (refer to section 4.1 Appendix A – RA04) as below and send the form to the RA as soon as is practical after the return of the Smartcard:

Form field	Entry for single sponsor administration
User Name	The name of the user receiving the Short-term Access Smartcard
User Smartcard UUID	The user's UUID
Short-term Access Smartcard Name	The naming convention on the card, i.e. SAS – Custodian Forename Custodian Family Name – Profile Identifier
Short-term Access Smartcard UUID	The UUID of the Short-term Access Smartcard
Reason for Issue	For example, a locum member of staff is booked at short notice
Start Date & Time	Start date and time should correspond to the issuance time
Return Date & Time	Return date and time should reflect the return time
Name (sponsor)	Sponsor name
Smartcard UUID (sponsor)	Sponsor UUID
Date completed (sponsor)	Date when the sponsor completed the form
Sponsor's signature	The sponsor must sign the form

There should be one RA04 for each usage of the Short-term Access Smartcard. The RA should collate these and these can be used to cross reference to any ERS audit trails should any Care Record Guarantee queries arise.

The standard Fallback log should not be utilised for use with a Short-term Access Smartcard as it is difficult to monitor and requires the RA to check these on a daily basis.

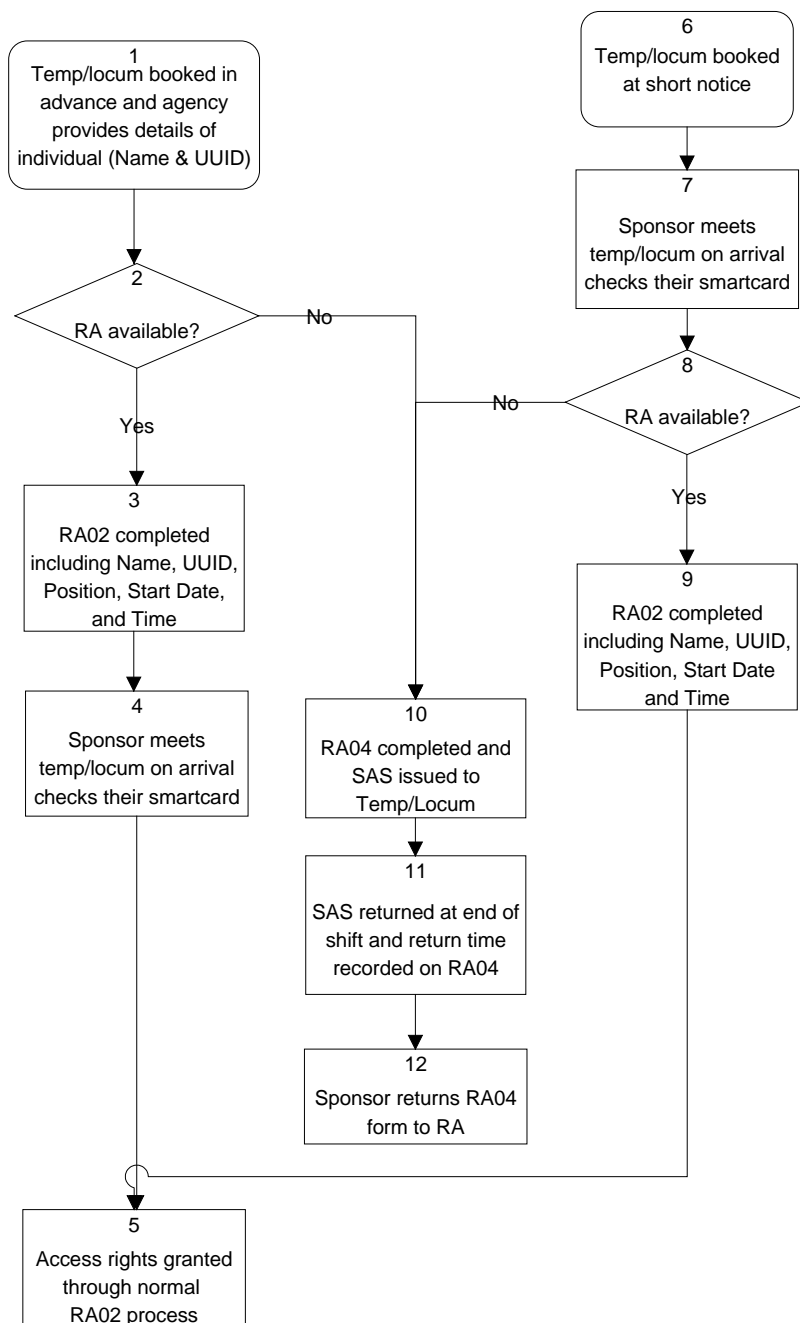
3.5 Audit

It is suggested that organisations may wish to develop an Ad hoc report within the ERS to monitor the usage of Short-term Access Smartcards and utilise this to reconcile the RA04 forms to usage and to investigate any disparity.

30th September 2008

3.6 Process for Assigning Short-term Access Smartcards

The flowchart below illustrates the process issuers will follow when assigning a Short-term Access Smartcard to healthcare workers.



Notes	Description
1	The agency needs to determine the UUID of the user. This may require dialogue with the Registration Authority.
4 & 7	A temporary or locum member of staff must first register for an NHS CRS Smartcard before access profiles can be allocated to them.
10	As for box 2, but for Short-term Access Smartcards the position should contain the name and UUID of the Short-term Access Smartcard. Short-term Access Smartcards are valid for 12 hours.

30th September 2008

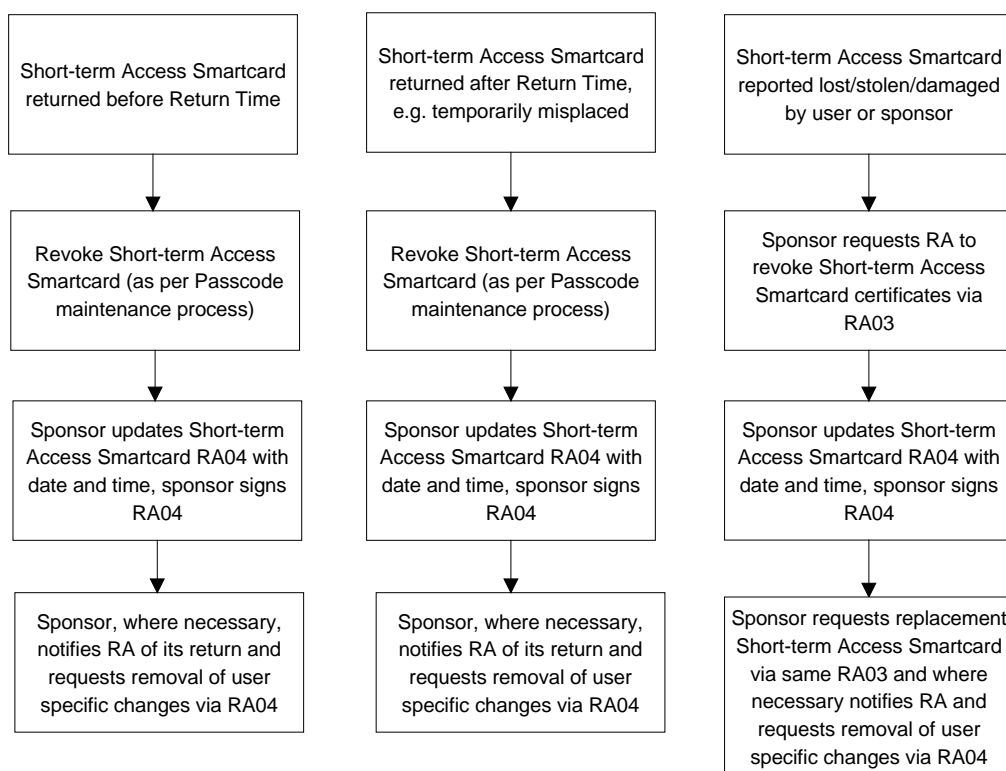
3.7 End of Usage Period

Short-term Access Smartcards should be returned to an appropriate issuer by the user on or before the return time (no greater than 12 hours from the time of issue). It is recommended that the issuer of the Smartcard locks the Smartcard when it has been returned. If the Smartcard is not returned at or before the return time the issuer should notify the RA of the failure to return the Smartcard. The RA will then remove the profile(s) associated with the Short-term Access Smartcard.

The RA will remove any user specific profiles granted to the Short-term Access Smartcard via the RA04, when the return time has expired or when notified the Short-term Access Smartcard has been returned early.

If the Short-term Access Smartcard is reported lost, stolen, or damaged the RA will revoke the Short-term Access Smartcard certificates.

3.8 Process for the Return of Short-term Access Smartcards



30th September 2008

4 Appendices

4.1 Appendix A – RA04

RA04 Form – Usage of or Change to Short-term Access Smartcard profile



Please note:

- o This form should be used to record the usage of or change the profile associated with, a Short-term Access (SAS) to be issued to an **authorised user who has been issued with their own Smartcard**.
- o Short-term Access Smartcards should only be issued to temporary or locum staff where there is a definite clinical or business need to access a NHS CRS application.
- o This form may be used to reconcile against usage.
- o This form can be completed online but must not be submitted online as it requires your signature.
- o When completed, print the RA04 form, sign and send to your local Registration Authority as soon as possible.

User Name		User Smartcard UUID	
Short-term Access Smartcard Name		Short-term Access Smartcard UUID	
Reason for Issue			
Start Date & Time		Return Date & Time	

Only complete the following 4 fields if the Smartcard requires a change to the profile

Organisation	Code	Action
Job Role	Code	Action
Area of Work	Code	Action
Activity	Code	Action

¹ Sponsor (Sponsor to complete below)		³ RA Agent/Manager (RA to complete below)
Name		
Smartcard UUID		
Date completed		

Sponsor's declaration:

I confirm, where recorded, that the **Organisation, Job Role(s), Area(s) of Work and Activity(ies)** detailed above are correct and should be applied by the Registration Authority to the Short-term Access Smartcard detailed above. AND/OR I have confirmed the identity of, and issued a Short-term Access Smartcard to the user above.

Sponsor's signature: _____ Date _____

Notes to Registration Authority:

¹Ensure you have verified the form has been completed by an appropriate Sponsor i.e. one who can approve the profile change being requested. If this is not the case then do not action and advise the requestor. If in doubt contact your RA Manager.

30th September 2008

4.2 Appendix B – RA09

RA09 Form – Creation of Self Service Fallback Smartcard



Please note:

- o This form should **only** be used to create a Fallback Smartcard to be issued to an **authorised user**.
- o This document can be completed online but must not be submitted online as it requires your signature.
- o When completed, print the RA09 form, sign and send to your local Registration Authority.
- o **Strike through all blank fields.**

¹ Custodian Name	Custodian Smartcard UUID

Fallback Smartcard Name	Fallback Smartcard UUID

Organisation	Code

³ RA Agent/Manager (RA to complete below)	
Name	
Smartcard UUID	
Date Completed	

Custodian declaration:

I confirm that the details in this RA09 form are correct and a self service Fallback Smartcard should be produced by the Registration Authority.

Custodian's signature: _____ Date _____

Notes to Registration Authority:

¹ Custodian need not be a sponsor but are responsible for the issuing of self service Fallback Smartcards as required

² Ensure you have verified the form has been completed by an appropriate custodian If this is not the case then do not action and advise the requestor. If in doubt contact your RA Manager.