
THE ELECTRONIC STAFF RECORD PROJECT



NATIONAL HEALTH SERVICE

M-3970 ESR NHS CRS SMARTCARD LOGIN ENABLEMENT IMPLEMENTATION GUIDE

Author: Chris Price
Owner: Stuart Fox
Creation Date: 01st September 2008
Last Updated: 29th June 2009
Version: v 2.3

Approvals:

Name	Stuart Fox
Title	RPP Project Manager
<hr/>	
Name	Lee Pacey
Title	NHS Development Manager
<hr/>	
Name	Colin Fincham
Title	Programme Manager, Access Control
<hr/>	

1. Document Control

1.1. Change Record

Date	Author	Version	Change Reference
01/09/08	Sean Murphy	0.1	Original Draft
16/09/08	Sean Murphy	0.2	Updates following initial early review
22/09/08	Sean Murphy	0.3	Updates following meeting
26/09/08	Sean Murphy	0.4	Updates following NHS internal review
07/10/08	Sean Murphy	0.5	Re-write following third review
29/10/08	Sean Murphy	0.6	Restructure and rewrite following NHS CFH review.
04/11/08	Sean Murphy	0.7	Updates following CFH review
11/11/08	Sean Murphy	0.8	Updates following final review
21/11/08	Sean Murphy	1.0	Formal Release
30/03/09	Chris Price	1.1	Updates following completion of the pilot phase
15/04/09	Chris Price	1.2	Further updates following pilot review
21/04/09	Chris Price	1.3	Further updates following review
21/04/09	Chris Price	2.0	Formal release following review
08/05/09	Chris Price	2.1	Update to section 5.8.1 Shared Service Staff and minor amendment to section 5.4
28/05/09	Chris Price	2.2	Amendments made following comments received.
29/06/09	Chris Price	2.3	Amendments relevant to Shared service Staff

1.2. Reviewers

Name	Position
Stuart Fox	RPP Project Manager
Lee Pacey	NHS Development Manager
Alexia Rothwell	NHS Data Projects Manager
Steve Thrussell	McKesson ESR Design Architect
Jane Siddle	McKesson Registrations Project Manager
Allan Morris	RPP Implementation Lead
Colin Fincham	Access Control Programme Manager
Kirstie Wilson	NHS CFH Access Control Guidance Manager

1.3. Distribution

Copy No.	Name	Location
1	NHS Library Master	NHS RPP Project Library
2		

2. Contents

1. Document Control	2
1.1. <i>Change Record</i>	2
1.2. <i>Reviewers</i>	2
1.3. <i>Distribution</i>	2
2. Contents	3
3. Introduction	4
3.1. <i>Background</i>	4
3.2. <i>Purpose</i>	4
3.3. <i>Scope</i>	4
3.4. <i>Definitions</i>	4
3.5. <i>Reference Documentation</i>	5
4. NHS CRS Smartcard Enablement: IT Requirements	6
4.1. <i>IT Pre-requisites</i>	6
4.2. <i>IT activities required during ESR NHS CRS Smartcard Implementation</i>	6
5. Registration Authority Requirements	7
5.1. <i>Step 1: Provide authority to the Central Team to extract data from NHS CRS</i>	7
5.2. <i>Step 2: Use ESR reports to identify all ESR users</i>	7
5.3. <i>Step 3: Allocate NACS code within ESR</i>	7
5.4. <i>Step 4: Issue NHS CRS Smartcard to ESR users who do not have an NHS CRS Smartcard</i>	8
5.5. <i>Step 5: Inform Central NHS ESR Data Team of all ESR users</i>	8
5.6. <i>Step 6: Provide data cleansing/matching reports to NHS organisations</i>	8
5.7. <i>Step 7: Data cleansing work completed by NHS organisations</i>	9
5.8. <i>Step 8: Additional considerations for shared service organisations</i>	9
6. ESR UUID Load and Maintenance	11
6.1. <i>Initial data load of NHS CRS data into ESR for ESR users</i>	11
6.2. <i>Ongoing maintenance of ESR NHS CRS UUID prior to ESR interface implementation</i>	12
7. Process Flow Diagrams	12
8. Appendix A – Reference Documentation	12

3. Introduction

3.1. Background

ESR (Electronic Staff Record) is the integrated Human Resources (HR) and Payroll system used by the NHS in England and Wales. All NHS organisations within England are moving to NHS CRS Smartcard facilitated ESR access as part of the drive to improve information governance for all personal identifiable data held by the NHS. This will provide ESR with the e-GIF Level 3 security required to effect changes on the NHS CRS through the forthcoming interface between both systems (functionality delivery expected end of August 2009). It will also ensure staff data is secured to the same level as patient data. NHS CRS Smartcards will need to be issued to all users of ESR, including Manager and Employee self service, ultimately this will be the only available method of accessing ESR.

HR functions currently update ESR when changes are made regarding an employee's assignment to an established position. The ESR interface will be triggered by such changes and will automatically update an individual's access rights to NHS CRS compliant systems, reflecting the requirements of their new position. It will enable the management of access control via a single point of data – the change to the employee's position within ESR.

The move to NHS CRS Smartcard access is scheduled to take place between May and August 2009.

3.2. Purpose

The purpose of this document is to explain the process required to transition all ESR users from the existing login process to using the NHS CRS Smartcard to access ESR. The primary audience is an organisations Registration Authority (RA) function although input will also be required from local HR departments, IT departments and ESR administrators.

3.3. Scope

This document is an implementation guide for an NHS organisation's HR and RA team. A number of activities referred to within this document will also require input and assistance from the local IT departments and ESR lead contact. The document is limited solely to the rollout of NHS CRS Smartcard login for ESR users.

The document will detail the steps required in order for an NHS organisation to move from existing username and password access arrangements to access via an NHS CRS Smartcard.

Updates to this document will be made in line with changes to strategy, process and technical design, as they are established throughout the project lifecycle.

3.4. Definitions

A number of acronyms are in use throughout this document and for reference a simple glossary follows to explain the system or function that each one represents:

e-GIF Level 3. Security standards for access to government systems. e-GIF (Government Interoperability Framework) Level 3 refers to policies and standards to enable information to flow seamlessly across the public sector and provide citizens and businesses with better access to public services.

ESR URP: User Responsibility Profile. Used within ESR to define the access rights a user has to specific areas of functionality and data.

IA: Identity Agent refers to the desktop software that authenticates a NHS CRS Smartcard to ensure the user is active and authenticated on NHS CRS.

NACS: National Administrative Codes Service. These are codes allocated by NHS Connecting for Health that provide a unique identification record for any organisational entity at almost any level, be that an NHS Trust or PCT, or one of its hospitals. Used by IT systems to identify locations reliably, quickly and easily. The NACS coding structure provides a picture of the NHS' organisational hierarchy, and the links between

the various organisations at different levels. Each VPD will have an equivalent NACS code at the highest organisational level.

NHS CRS: The NHS Care Records Service will help NHS organisations in England to store patient health care records on computers that will link information together quickly and easily. An NHS CRS Smartcard will give a user access to the NHS CRS and other National Programme for IT (NPfIT) applications such as Choose and Book and the Electronic Prescription Service.

NHS CRS Smartcard: A plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access the NHS CRS and other NPfIT applications, along with a Passcode. The chip does not contain any personal information. The combination of the NHS CRS Smartcard and Passcode together provide high levels of security and confidentiality.

NHS organisation: Any organisation using ESR will be referred to as an “NHS organisation” within this document. This can be any single entity that translates to a unique VPD within ESR. It is recognised that one NHS organisation can support several other NHS organisations, in particular in a shared service environment. To that end, updates or process changes required on ESR should be applied to each individual VPD within an NHS organisation or shared service managed group. Each ESR VPD will have an equivalent NACS code at the highest Organisational level.

SUD: Spine User Directory is the repository which stores users’ profiles and registration information both current and historic e.g. includes roles and organisations that an individual works for.

UIM: User Identity Management is the new registration software which will provide the electronic management of access control which is replacing the current paper based registration process (expected to be available in late 2009).

UUID: The User’s Unique ID Number is used by all NPfIT applications to uniquely identify the user to the application. The UUID is the number displayed on the NHS CRS Smartcard. Occasionally called the UID (Unique ID Number). ESR will also hold the NHS CRS UUID against employee records so that it can validate that the employee has an active registered entry on NHS CRS.

VPD: Virtual Private Database is a database security facility developed within the ESR application. Each of the 586 NHS organisations using ESR use exactly the same application over the same database at the same time, but can only see the employee data relating directly to their individual organisation.

NHS CRS Data: Data that is received from the SUD will be referred to as NHS CRS data. In the context of this document this is limited to:

- When a user inserts their NHS CRS Smartcard, the ESR Smartcard login functionality will use Identity Agent software to validate that they are a registered and active user on NHS CRS before allowing entry to ESR.
- The NHS CRS extract data that is used for populating the NHS CRS UUID within ESR.

3.5. Reference Documentation

For details on the NHS CRS to ESR Data Matching requirements please refer to the latest version of the document “NHS CRS to ESR Matching User Guidance” referenced within [Appendix A](#).

4. NHS CRS Smartcard Enablement: IT Requirements

There are a number of IT related activities that need to be undertaken by organisations prior to and during the NHS CRS Smartcard enablement implementation.

4.1. IT Pre-requisites

As part of the upgrade of the ESR service, there is a requirement for all NHS organisations to transition from using J-initiator to Sun JRE. Upgrading to JRE version 1.6.0_06 is a pre-requisite to using NHS CRS Smartcards.

4.1.1. Java Runtime Environment (JRE) download to desktops of ESR users

Organisations must have the recommended version of JRE (version 1.6.0_06) installed on their PCs prior to the enablement of NHS CRS Smartcards as communicated via ESR User Notice 957 (Document *M-0250 JRE Deployment Guide* within appendix A provides further details regarding the JRE installation/configuration requirements). The entry of the NHS CRS UUID (users unique ID number) into ESR, which is undertaken as part of an organisations Smartcard implementation activities, will trigger ESR to initiate JRE for a particular user. Therefore JRE must be installed onto PCs prior to the UUID being entered into ESR.

The following web page provides information on the current level of JRE running on the PC and a link to the *M-0250 JRE Deployment Guide*: <http://www.esrsupport.co.uk/rpp/>.

Organisations are strongly recommended to ensure their local IT department is aware of the JRE requirement immediately as per ESR User Notice 957.

4.2. IT activities required during ESR NHS CRS Smartcard Implementation

The following additional IT related activities will need to be undertaken during the ESR NHS CRS Smartcard implementation.

4.2.1. Installation of ESR NHS CRS Smartcard reader and Identity Agent software on local user PC

For the rollout of ESR NHS CRS Smartcard login, all ESR users must have an NHS CRS Smartcard reader, and Identity Agent software installed on their PC prior to NHS CRS Smartcard issuance.

During the installation of the Identity Agent Software reference must be made to the **JRE configuration steps** provided within the Identity Agent Installation Guide (the guide is downloaded with the software). **These steps must be followed in order for ESR access via NHS CRS Smartcard to be successful** (The M-0250 JRE Deployment Guide also refers to this essential JRE configuration).

Organisations are strongly recommended to ensure their local IT Department are aware of this JRE configuration requirement during the IA software installation.

For further information regarding NHS CRS Smartcard hardware/software refer to:

- Practical Essentials on the RA website:
<http://www.connectingforhealth.nhs.uk/implementation/registrationauthorities/practical-essentials>.
- RA Hardware Ordering and Returns Process:
<http://www.connectingforhealth.nhs.uk/implementation/registrationauthorities/practical-essentials/equipment>

4.2.2. Amend URL for NHS CRS Smartcard access

When using an NHS CRS Smartcard to access ESR users must use a different URL dedicated to NHS CRS Smartcard access. Consequently desktop shortcuts/web portals will need to reference the URL specified below following the enablement of NHS CRS Smartcards.

https://esr.mhapp.nhs.uk/OA_HTML/xxnhs/smartcard/esrSmartcardLauncher.jsp

Until the NHS CRS Smartcards are implemented within an organisation the existing URL should continue to be used.

https://esr.mhapp.nhs.uk/oa_servlets/AppsLogin

4.2.3. Access to an @nhs.net e-mail account

During the ESR NHS CRS Smartcard implementation data cleansing/matching reports will be delivered to each organisation (please refer to section 5 for further details). In the interests of data security these reports must be delivered to an @nhs.net e-mail account. Consequently there is a requirement for each organisation to identify an employee(s) who will receive the data/cleansing matching reports and ensure they have access to an active @nhs.net e-mail account.

5. Registration Authority Requirements

This section details the implementation steps to be undertaken by local RAs. Additional assistance will be required from ESR users with HR access rights.

Step 1: Provide authority to the Central Team to extract data from NHS CRS.

Step 2: Use ESR reports to identify all ESR users

Step 3: Allocate NACS code within ESR

Step 4: Issue NHS CRS Smartcard to ESR users who do not have an NHS CRS Smartcard

Step 5: Inform Central NHS ESR Data Team of all ESR users

Step 6: Provide data cleansing/matching reports to NHS organisations

Step 7: Data cleansing work completed by NHS organisations

Step 8: Additional considerations for shared services organisations

5.1. Step 1: Provide authority to the Central Team to extract data from NHS CRS

During the NHS CRS Smartcard implementation it will be necessary for the NHS ESR data team to access data held on NHS CRS. Prior to a data extract being taken permission must be obtained from the NHS organisations RA manager or HR director (this permission will be used for NHS CRS data extracts required throughout the implementation). A suggested template of this permission will be e-mailed to organisations during the early stages of implementation. It is imperative that permission is granted as soon as possible so that the matching process described in **Step 6: Provide data cleansing/matching reports to NHS organisations** can be initiated in a timely manner.

5.2. Step 2: Use ESR reports to identify all ESR users

All existing ESR users must be identified so that they can be issued with an NHS CRS Smartcard. The standard ESR report 'NHS Active Responsibilities' should be used to identify all users by their ESR URP. This can be run by any user with one of the following ESR URPs: Local HRMS Systems Administration, Local HRMS Systems and User Administration, and Local HRMS User Administration. **A user with the Local HRMS Systems and User Administration URP should also check that each user profile is linked to the correct person record within ESR.**

The list of ESR users should then be submitted to the HR/RA teams and the NHS ESR Data Team. The list of ESR users should also be forwarded onto the local IT department to ensure they are aware of all users that may require amendments to their desktop configuration as specified within Section 4 "NHS CRS Smartcard Enablement: IT Requirements".

5.3. Step 3: Allocate NACS code within ESR

Whereas ESR maintains a Trust Identifier, NHS CRS uses a NACS code to identify NHS employing organisations. For the purposes of communication between ESR and NHS CRS only the NACS codes relating to 'top-level' organisations are required. This is typically at the trust level but in some circumstances a single trust within ESR administers multiple NACS codes (where organisations have merged for instance).

It is essential for an organisation's workstructures administrator to assign the correct NACS code before deploying NHS CRS Smartcards. The "CRS Organisation NACS Code" field on the "Add'l Org Unit Details" screen will hold the NACS code value and can be selected from an LOV (List of Values). NHS organisations can view their NACS details at:

<https://www.nhs.uk/ods/>

5.4. Step 4: Issue NHS CRS Smartcard to ESR users who do not have an NHS CRS Smartcard

Any ESR users identified in section 5.2 who do not have an existing entry on the SUD must have their identity checked to e-GIF Level 3, have a personal record created in the SUD as per the usual RA registration process, before being issued with an NHS CRS Smartcard. During the creation of a SUD entry each ESR user will be allocated a UUID which as well as uniquely identifying a user to an NHS CRS application, is also the key data item that will control a user's ESR access via an NHS CRS Smartcard and link their ESR employee record to the SUD.

The SUD entry, whether this has been created or was already present within NHS CRS, must be associated to the organisation. The access is provided by linking the UUID between ESR and the SUD, and the ESR access rights are determined within the ESR system. The Identity Agent (IA) logon authentication process requires a Role or Activity to be present within the SUD but there is no Role or Activity specifically for ESR access. Consequently, the Activity or Role of R8008 should be used (as this has no other baseline activities associated with it), unless the user has an existing Role (and Area of Work or Additional Activities) for access to NHS CRS applications: these should not be altered.

5.5. Step 5: Inform Central NHS ESR Data Team of all ESR users

The NHS ESR Data Team will supply the NHS organisation with a spreadsheet to be populated with details of the ESR users. The details, which should include the UUID of ESR users identified by the NHS Active Responsibilities report, must be returned to the Data Analyst in the NHS ESR Data Team (via an @nhs.net email address) who is an appointed contact for the NHS organisation.

The NHS ESR Data Team will take the user report as a basis as they oversee the automated process for populating the SUD UUID against the ESR users person record (refer to section 6 "ESR UUID Load and Maintenance").

5.6. Step 6: Provide data cleansing/matching reports to NHS organisations

The NHS ESR Data Team will produce a set of Excel reports that provide assurance to the NHS organisation that their user data in ESR correctly 'joins' to the same user data in NHS CRS. This free service is purely to assist NHS organisations to improve data quality; therefore supplied reports are for information and may require the NHS organisation to action. The reports will detail all ESR users with exact 'matches' for reference, those that have failed to match are divided into a number of different categories (refer to M-3980 NHS CRS to ESR Matching User Guidance within [Appendix A](#)).

This exercise will ensure that the correct NHS CRS UUID is entered against the correct ESR person record. For this reason it is in the interest of the NHS organisation to ensure as many ESR users are correctly matched between the two systems prior to the UUID data load.

For reference, the data fields used in the matching process are National Insurance number, First Name and Family Name.

The NHS CRS to ESR data matching process consists of the following stages:

1. The NHS ESR Data Team will request permission to extract NHS CRS data from the RA Manager or HR Director.
2. Once permission is received, the data will be extracted directly from the SUD.
3. An extract will be taken from ESR.
4. The ESR user list provided in section 5.5 (**Step 5**) will be used to generate a subset of records which will be matched from the NHS CRS and ESR extracts supplied.
5. A set of 'cleansing' reports will be produced and provided to the NHS organisation for action.

For further clarity regarding these steps please refer to the flow charts at [Section 7](#).

5.7. Step 7: Data cleansing work completed by NHS organisations

Following receipt of the cleansing reports, the RA/HR teams can assess in the case of mismatches whether ESR or NHS CRS holds the correct information, and if required update the relevant application accordingly. **e-GIF Level 3 identity verification must be adhered to for changing NHS CRS data in order to maintain compliance with the e-GIF Level 3 standard.**

Please see the Data Cleansing User Guidance in [Appendix A](#) for details of the data cleansing process.

It is expected that all ESR users will be matched within tolerances agreed with the NHS organisation following advice from the NHS ESR Data Team. The definition of tolerances will be influenced by the reports produced by the NHS ESR Data Analysts; these should be achieved before data can be loaded into ESR. The cleansing work will be overseen and monitored by the NHS ESR Data Team. Precautionary advice will be given to any NHS organisation with a volume of mismatch deemed, by the appointed Data Analyst, to be potentially detrimental to the success of NHS CRS Smartcard rollout.

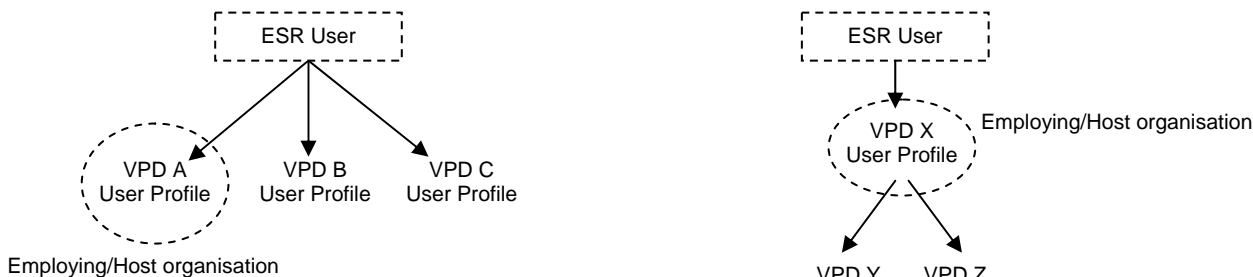
The NHS organisation will be responsible for ensuring that all of their ESR user person records are cleansed to a satisfactory level and in line with the guidance within [Appendix A](#) (M-3980 NHS CRS to ESR Matching User Guidance).

5.8. Step 8: Additional considerations for shared service organisations

Special consideration must be made for organisations that support, or are part of a shared service group. The UUID entry may vary depending on the way users within the shared service group currently login to ESR. Currently a user may access multiple VPDs using separate usernames and passwords or may access multiple VPDs using a single username and password (ESR shared service single sign-on). This is depicted below:

(a) Separate usernames and passwords

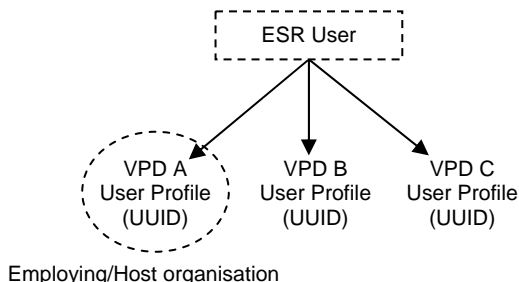
(b) Single username and password



5.8.1. Separate usernames and passwords

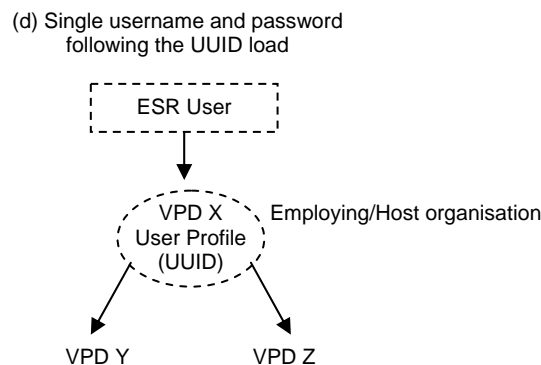
In certain situations employees will exist as active users in more than one ESR VPD and will login to ESR using **separate** usernames and passwords for each VPD (i.e. a user profile at each VPD). To enable NHS CRS Smartcard access to ESR they will need a person record **in every ESR VPD in which they are a user**. Where person records do not already exist for these users they should be created with the new person type of “External Shared Service Staff” and then linked to the relevant user profile. This will allow the necessary NHS CRS UUID to be entered against the person record, which provides the authentication link to the NHS CRS system to allow NHS CRS Smartcard access. This is presented diagrammatically below:

(c) Separate usernames and passwords following the UUID load



5.8.2. Single username and password

Alternatively shared service staff may have access to multiple VPDs using their host organisation username/password. In this scenario it will only be necessary to enter the UUID against the person record at the host organisation (i.e. the organisation where they have a user profile to log into ESR). This will provide access to URPs in the same way as the existing username and password login. This is presented diagrammatically below:



In all cases shared service employees will need to be entered onto the SUD and will therefore have to be identity verified to e-GIF Level 3. This requirement is the responsibility of the RA to provide support to the shared service supplier.

5.8.3. External Shared Service Staff person type

The “External Shared Service Staff” person type does not require the same mandatory data items to be populated within ESR as necessary for the “Employee” person type. The “External Shared Service Staff” person type has been created to facilitate the entry of the UUID into ESR where a person record does not currently exist for the user.

As the “External Shared Service Staff” person type is not treated as an employee record within ESR, and therefore can be created with minimal information, it is not possible to load the UUID into ESR as part of the automated data load performed by the NHS ESR data team. The UUIDs for shared service staff should however be included within the ESR user template spreadsheet (refer to “*Step 5: Inform Central NHS ESR Data Team of all ESR users*”) as this will ensure the UUIDs and associated information for all ESR users has been identified. Following the data load the UUIDs for “External Shared Service Staff” will be reported back to the organisation (if they were included within the ESR user template spreadsheet submitted to the NHS ESR data team) for manual entry into ESR. This activity should be co-ordinated with the shared service provider.

5.8.4. NHS Shared Service Providers

The following key points are relevant to NHS organisations that support, or are part of an NHS shared service group:

- When a UUID has been entered into ESR the associated user will be able to access ESR via their NHS CRS Smartcard.
- ESR users will not be able to adopt full use of their NHS CRS Smartcard for multiple VPD access until the same NHS CRS UUID has been loaded against each user’s person record within ESR.
- If UUID loads have not been completed at each VPD the user will temporarily have NHS CRS Smartcard access to one VPD and traditional username/password access at another. **The NHS Central team therefore strongly recommends that the transition to NHS CRS Smartcard access for all client organisations of the shared service provider is co-ordinated to utilise the same data load slot.**
- Where the users included within a UUID load are based at another organisation (e.g. an organisations UUID load may include users that are based at a shared service provider) the implementation activities must be co-ordinated by the organisations that are part of the shared service arrangement. This will ensure all users included within the UUID load are able to access ESR via their NHS CRS Smartcard.
- Following the entry of the UUID against a person record, ESR will attempt to initiate JRE rather than J-Initiator the next time the user accesses ESR. If all VPDs to which the user has access have not performed the UUID load it is possible users will be signing into ESR at a VPD that **has loaded their UUIDs** (in this case ESR would initiate JRE) and may also be manually signing into other VPDs that **have not loaded their UUIDs** (in this case ESR would initiate J-Initiator).
- In the above scenario ESR users should ensure that they access ESR via separate internet explorer browser sessions which will allow JRE and J-initiator to run concurrently. Separate browser sessions can be initiated by selecting Internet Explorer from the Start menu for each ESR session that is

required. The first time that JRE is initiated the user will be presented with a dialogue box requesting verification that the application should be run. ESR users should click 'run' when prompted.

- Shortly after the UUID load access to ESR via the traditional login screen will be disabled, from this point forward access will only be possible by NHS CRS Smartcard.

5.8.5. Third Party Shared Service Providers (Non-NHS organisation)

The following key points are relevant to organisations that support, or are part of a third party shared service arrangement:

- Where NHS organisations utilise a third party shared service provider the UUIDs for all users reported by the Active Responsibilities report (including external shared service employees) should be included within the ESR user template that is submitted to the NHS ESR data team as part of an organisations implementation activities.
- When a UUID has been entered into ESR the associated user(s) will be able to access ESR via their NHS CRS Smartcard.
- ESR users will not be able to adopt full use of their NHS CRS Smartcard for multiple VPD access until the same NHS CRS UUID has been loaded against each user's person record within ESR.
- If the entry of UUIDs has not been completed at each VPD the user will temporarily have NHS CRS Smartcard access to one VPD and traditional username/password access at another.
- Following the entry of the UUID against a person record, ESR will attempt to initiate JRE rather than J-Initiator the next time the user accesses ESR. If all VPDs to which the user has access have not performed the UUID load it is possible users will be signing into ESR at a VPD that **has loaded their UUIDs** (in this case ESR would initiate JRE) and may also be manually signing into other VPDs that **have not loaded their UUIDs** (in this case ESR would initiate J-Initiator).
- In the above scenario ESR users should ensure that they access ESR via separate internet explorer browser sessions which will allow JRE and J-initiator to run concurrently. Separate browser sessions can be initiated by selecting Internet Explorer from the Start menu for each ESR session that is required. The first time that JRE is initiated the user will be presented with a dialogue box requesting verification that the application should be run. ESR users should click 'run' when prompted.
- When an organisation completes a UUID load that includes third party shared service users the implementation activities **must** be co-ordinated by the client organisation and the third party shared service provider. This will ensure all users included within the UUID load are able to access ESR via their NHS CRS Smartcards. The Shared Service provider should also be aware of the potential JRE/J-Initiator conflicts following the entry of the UUID and must therefore co-ordinate the implementation activities with client organisations accordingly.
- Shortly after the UUID load access to ESR via the traditional login screen will be disabled, from this point forward access will only be possible by NHS CRS Smartcard.

6. ESR UUID Load and Maintenance

To ensure that the ESR and NHS CRS are correctly aligned in respect of ESR user entries; the following two requirements must be enforced to maintain data integrity:

- Initial data load of NHS CRS Data into ESR for ESR users
- Ongoing manual maintenance of ESR NHS CRS UUID

6.1. Initial data load of NHS CRS data into ESR for ESR users

In order for ESR users to begin using their NHS CRS Smartcards (assuming these have been produced in **Step 4: Issue NHS CRS Smartcard to users**) the UUID must be populated against the ESR person record. The initial population of NHS CRS data into ESR will be controlled by the NHS ESR Data Team.

As part of the data matching tool developed by the NHS ESR Data Team, an option exists that can be selected to produce a file that can be loaded into ESR. A number of the stages detailed in section 5.6 "*Step 6: Provide data cleansing/matching reports to NHS organisations*" (1 to 4) will be repeated as part of the upload file creation. The UUID will therefore be populated in ESR through the following stages:

1. The user list provided in section 5.5 **Step 5: Inform Central NHS ESR Data Team of all ESR users** will be used to generate a subset of records which will be matched from the NHS CRS and ESR extracts supplied.

2. The matching utility (operated by the NHS ESR Data Analyst) will produce a file based on the exact matches made between the ESR and NHS CRS extract files. The file will contain the ESR employee number and the UUID.
3. The upload file will be placed into a secure folder on the McKesson¹ network.
4. A request will be initiated that retrieves the upload file and loads the UUID against the related ESR Person record.
5. An exception report will be produced detailing any records that have failed to load, this will be passed to the NHS organisation to address.

Prior to the UUID being populated within ESR (whether this be via the data load or manual entry) an organisations HR/RA personnel should be satisfied that the prerequisites to NHS CRS Smartcard enablement have been met.

6.2. Ongoing maintenance of ESR NHS CRS UUID prior to ESR interface implementation

It is recognised that there may be a time difference of several months between an NHS organisation issuing NHS CRS Smartcards to users, and the ESR interface to UIM being implemented. Prior to the interface functionality being delivered, intended for the end of August 2009, any new users (i.e. new starters that did not have their UUID loaded into ESR by the NHS ESR Data team) within the NHS organisation will need to be manually entered directly into NHS CRS and ESR. The task of entering the UUID into ESR will be restricted to the ESR user allocated the Local HRMS Systems and User Administration URP.

WARNING: It is critical that the correct UUID is manually entered against the ESR user's person record within ESR. If an incorrect value is entered then it may be possible for the employee to sign on as a different employee (if their UUID value is the same as the incorrect value entered) which is a serious breach of security. It is strongly recommended that this data entry is verified by a second person prior to committing to the ESR Database.

Following the delivery of the ESR interface to UIM functionality all manual maintenance will be replaced with a search facility from ESR to locate the equivalent NHS CRS record. Any ESR users that may have been missed from the initial data load will need to have the data items manually entered against their person records as described above. Shortly after the UUID load access to ESR via the traditional login screen will be disabled, from this point forward access will only be possible by NHS CRS Smartcard.

7. Process Flow Diagrams

Process Flow diagrams have been produced to detail the stages within this document at a pictorial level. These are separately controlled documents and are available via <http://www.esrsolution.co.uk/iim/>

The flowchart document references are:

NHS organisation SMARTCARD Implementation – 1
NHS organisation SMARTCARD Implementation – 2

8. Appendix A – Reference Documentation

“M-3980 CRS to ESR Matching User Guidance”
“M-0250 JRE Deployment Guide”

The latest version of the documentation referenced above can be found via the following URL

<http://www.esrsolution.co.uk/iim/>

¹ McKesson, in partnership with the NHS, host and support the ESR application