# Registration Authority Policy

## Document Reference

<table>
<thead>
<tr>
<th>Directorate / Programme</th>
<th>Interoperability &amp; Architecture</th>
<th>Project</th>
<th>NHS Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programme / Project Manager</td>
<td>Philip Gill</td>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Owner</td>
<td>Andrew Meyer</td>
<td>Version</td>
<td>2.4</td>
</tr>
<tr>
<td>Author</td>
<td>Philip Gill</td>
<td>Issue date</td>
<td>22 May 2020</td>
</tr>
</tbody>
</table>
Document Management

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.1</td>
<td>5 March 2019</td>
<td>Includes new identity verification standards and policy approval for additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authentication methods that meet approved standards</td>
</tr>
<tr>
<td>2.4</td>
<td>22 May 2020</td>
<td>Includes virtual smartcards, authorised devices and iPad as a category of authentication methods permitted by NHS Digital</td>
</tr>
</tbody>
</table>

Reviewers

This document has been sent to for review and/or reviewed by the following people (please include nil returns):

<table>
<thead>
<tr>
<th>Reviewer Name</th>
<th>Title / Role / Directorate</th>
<th>Version</th>
<th>Date Sent to Reviewer</th>
<th>Date Feedback Received</th>
<th>Feedback Actioned (Y/N ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike Walker</td>
<td>Programme Head – Integrating Care</td>
<td>2.4</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Hazel Randall</td>
<td>Head of Legal</td>
<td>2.4</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Mike Partridge</td>
<td>National RA Manager</td>
<td>2.4</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Andy Smith</td>
<td>Principal Security Specialist</td>
<td>2.4</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

*This document must be quality assured by the Directorate PMO before approval by the SRO and NHS Digital Executive Portfolio Director before submission to the NHS Investment Sub-Group.

Approved by

This document has been approved by the following people:

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Title</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gareth Thomas</td>
<td></td>
<td>Senior Responsible Owner (SRO)*</td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>Andrew Meyer</td>
<td></td>
<td>Executive Portfolio Director*</td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>Mike Walker</td>
<td></td>
<td>Programme Head</td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>Philip Gill</td>
<td></td>
<td>Portfolio Item Manager</td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>NHS Identity Project Board</td>
<td></td>
<td></td>
<td></td>
<td>2.4</td>
</tr>
</tbody>
</table>

*This document must be approved by the SRO and relevant NHS Digital Executive Portfolio Director.

Glossary of Terms

<table>
<thead>
<tr>
<th>Term / Abbreviation</th>
<th>What it stands for</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>AAL</td>
<td>Authentication Assurance Level</td>
</tr>
<tr>
<td>NHS Identity</td>
<td>Strategic Identity Service for health &amp; social care created as part of NIB 2020</td>
</tr>
<tr>
<td>FIDO</td>
<td>Fast Identity Online</td>
</tr>
</tbody>
</table>
**Document Control:**

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.
# Contents

1 **Introduction**  
   1.1 Purpose of Document  
   1.2 Background  

2 **Registration Authority Hierarchy**  

3 **Creation of a national digital identity**  

4 **Roles & Responsibilities**  

5 **Requirements in relation to Smartcards and other approved devices and authentication methods**  

6 **Local RA Policy**  

7 **Failure to comply with policy requirements**  

Appendix 1 – RA Manager Responsibilities  

Appendix 2 – RA Agent Responsibilities  

Appendix 3 – Sponsor Responsibilities
1 Introduction

1.1 Purpose of Document

National IT systems for health need to ensure that users of these systems are identified correctly and are given appropriate access. This is achieved by identity verification and creating a national digital identity for each user wishing to access the NHS Care Records Service\(^1\), using the Care Identity Service provided by NHS Digital. The process to doing this uses local ‘Registration Authorities’ (with delegation from NHS Digital) which consist of organisations with people and processes who are trained to create identities and grant access for themselves and other organisations in their area. This policy covers these services and the terms on which organisations may act as a local Registration Authorities and/or use the Care Identity Service.

This policy replaces the Registration Authority Policy Version 2.31 issued on 5 March 2019.

As part of the NHS Identity Project, this Registration Authority (RA) policy requires updating to ensure that it supports the modern delivery of health and social care across boundaries and in multiple locations whilst ensuring staff have access to appropriate, up to date, clinical information at the point of need. Details of the project aims and developments can be found at [https://digital.nhs.uk/services/nhs-identity](https://digital.nhs.uk/services/nhs-identity). The key elements of the policy that have been updated in this version 2.4 relate to:

- Providing details of different Authentication Tokens available, and how these may be issued and used.

This document lays out the RA policy requirements which every organisation that is or has a Registration Authority needs to adhere to. It is based on the original Department of Health (DH) Gateway document (reference number 6244) ‘Registration Authorities: Governance Arrangements for NHS Organisations’, the NHS Care Record Guarantee, GDPR requirements, and RA good practice guidance. Additionally the policy now reflects current best practice around Identity & Access Management as informed by the National Cyber Security Centre which covers what needs to be considered in identity verification and security requirements in relation to authentication to clinical systems and other systems which hold personal information. In particular this includes:


1.2 Background

This document outlines:

\(^1\) NHS Care Records Service applications includes the following: EPS, GP to GP, GPes, GpITF, NHS e-RS, SCR, SUS+, Spine CIS, Spine NHS Identity. See [https://digital.nhs.uk/services/](https://digital.nhs.uk/services/)

To note not all Authentication Tokens are recommended for access to EPS, only those that also constitute an ‘advanced electronic signature’.
• The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.
• The requirements for creating a nationally verified digital identity.
• The roles and responsibilities within organisations that run their own Registration Authority activity.
• Requirements in relation to authentication, and authentication methods for the different Authentication Tokens.
• The requirement to develop and implement a local RA policy.

1.3 Terminology

“Authorised Devices” means an alternative to smartcards, a device as approved by FIDO 2 Consortium that provides Assured Level 3 Authentication.

“Data Protection Laws” means applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including Regulation (EU) 2016/679, ‘the General Data Protection Regulation’ (“GDPR”) and the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, data protection authorities and other applicable Government authorities;

“Authentication Token” means Physical Smartcards, Virtual Smartcards, Authorised Devices and iPad Devices which enable healthcare professionals to access clinical and personal information appropriate to their role and the type of Identity Solution.

“iPad Device” means a tablet computer developed by Apple

“Physical Smartcards” means an approved physical card. Physical Smartcards are supplied by the authorised supplier(s) of cards to NHS Digital and are similar to chip and PIN bank cards.

“RA Agent” means an individual who has undertaken appropriate training who is authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user. In addition, they can perform a range of administrative tasks to maintain good RA records and processes

“RA Agent ID Checker” means an individual who has undertaken appropriate training who is authorised to undertake identity verification and identity creation.

“RA Manager” means an individual appointed by the Executive Management Team of an organisation to set up and run the organisations Registration Authority processes and procedures. In addition, they are responsible for ensuring good governance and report annually to the organisation’s EMT on RA activity. In addition, they are required to

---

2 These additional authentication methods must meet the National Institute of Systems and Technology (NIST SP800-63 Digital Identity Guidelines, available at https://pages.nist.gov/800-63-3/), this describes the cryptographic strength of authentication methods that is required to access special category data. In addition, devices and authentication methods need to meet FIDO 2 standards for how devices utilise the required cryptography (available at https://fidoalliance.org/) and must be accredited by the FIDO alliance.
undertake appropriate training to discharge these responsibilities and arrange training for all other RA team members. They are also authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user.

“Registration Authority (RA)” means NHS Digital as the single national Registration Authority and all other organisations that run a local Registration Authority on a delegated authority basis from NHS Digital.

“Sponsor” means an individual appointed by the Executive Management Team of an organisation who is authorised to request and approve that digital identities be created and appropriate and specific access assigned to staff within the organisation.

“Virtual Smartcards” means a solution that provides access functionality, but the card itself may be stored on a device, approved for use by NHS Digital and or its partners.

2 Registration Authority Hierarchy

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (NHS Digital). All organisations that run a local Registration Authority do so solely on a delegated authority basis from NHS Digital.

As NHS Digital is the single Registration Authority it needs to assure itself that organisations are operating appropriately and discharging their duties in an effective and consistent fashion. This policy outlines the minimum national requirements to provide such assurance: as such deviation from this policy document due to a local preference is not permitted. In addition, RA Managers are required to read and comply with RA operational guidance available at https://digital.nhs.uk/services/registrationAuthorities-and-smartcards

The original DH Gateway document (DH 6244) ‘Registration Authorities: Governance Arrangements for NHS Organisations’ outlines some of the requirements for delegated authority to local organisations to run their own RA activities and/or be a Registration Authority, for both their own users and users in other local organisations.

This policy document outlines the full range of mandatory requirements for an organisation to carry out this activity. The mandatory requirements in relation to organisational set up and appropriate governance oversight are:

1. There needs to be a Board/Executive Management Team (EMT) level individual who has overall accountability in the organisation for RA activity. The responsible individual must report annually to the organisation on this activity.

2. RA Managers are appointed by the Board/EMT and this appointment is confirmed in an official document (e.g. minute, letter of appointment, email from SRO etc.) which must be held by each individual appointed to these positions, and be made available for inspection when required.

3. RA Managers within organisations running their own RA activity are accountable for the running of RA activity in their organisation. They need to set up the systems and processes that ensure that the policy requirements contained in this document are met and local processes meet these requirements and cater for local organisational
circumstances (NOTE: deviation from these policy requirements due to a local preference is not permitted).

4. RA Managers and Agents need to keep up to date with national policy requirements, initiatives and changes. In order to do this, it is mandatory that their email address is entered as part of their personal details held within the database of registered users (The Spine User Directory).

5. RA Managers have a line of professional accountability to uphold good RA practice to NHS Digital.

6. The Registration Authority and, where different, employing organisation must:
   - have sufficient governance, processes and oversight in place to comply with the Data Protection Laws, including (but not limited to) providing fair processing information to all users, the NHS Code of Practice on confidential information, as amended from time to time, and the Care Record Guarantee; and
   - be registered for the Data Security Protection Toolkit and have a current latest status rating of at least ‘standards met’.

3 Creation of a national digital identity

NHS Digital’s strategic aim is to create a single, non-repudiated, trusted, digital identity for healthcare workers. This will be pivotal to enabling national access to health information in a secure way.

NHS Digital, as the single Registration Authority for health and social care, needs to be assured that users who have a digital identity created are subject to the same minimum standards of identity verification, to prove the individual has ownership of the identity irrespective of which local Registration Authority creates the identity. This is vital as the identity created is a national identity and must be trusted by each organisation where an individual is required to access the National Spine to access data. To achieve this, identity is required to be verified to the National Cyber Security Centre Good Practice Guide 45 – 'Identity Proofing and Verification of an Individual'. This provides assurance that the identity is valid across any organisation an individual works within.

In order to ensure this, the following requirements in creating a digital identity are mandatory. Registration Authorities, and, where different, the individual’s employing organisation must ensure that the following requirements are met:

1. Identity must be verified in a face to face meeting. It must be done by examining original identification evidence documents and seeing that identity relates to the individual who presents themselves at the meeting.

2. The person verifying the identity must be trained to do so. In Registration Authority terms this means that individuals holding the roles of RA Managers and RA Agents must perform these checks at face to face meetings since part of their responsibilities and requirements are that they are trained to carry out this activity. The RA Manager is responsible for training all other RA staff who will conduct ID checking to ensure that appropriate standards exist, and they can evidence good ID checking as part of the Data Security Protection Toolkit requirements.
The documents that can be used to verify an identity have been jointly determined by NHS Digital and NHS Employers and the list is contained in the NHS Employers ‘Verification of Identity Checks’ standard which can currently be found at [https://www.nhsemployers.org/your-workforce/recruit/employment-checks/identity-checks](https://www.nhsemployers.org/your-workforce/recruit/employment-checks/identity-checks). However GPG 45 processes and NHS Employers guidance, around managed risk, allow for additional documents to be considered provided they meet the GPG45 evidence category requirements.

3. Any changes to a person’s core identity attributes (Name, Date of Birth or National Insurance Number) need to go through the same face to face check with a person holding an RA role and provide appropriate documentary evidence.

4. Use of Authorised Devices and iPad Devices must be subject to the local Registration Authority’s and, where different, employing organisation’s device management policies (which should include additional relevant provisions where users are allowed to use their own personal devices for work purposes), and checks that the Authorised Device meets the minimum required solution specification.

5. Authentication Tokens can only be issued to individuals who have a national verified digital identity. This is also the case for processes that are used to issue temporary access to an individual – they need to have a verified identity first.

6. Different types of Authentication Tokens meet different levels of security classification. For further information see [https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities](https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities). The local Registration Authority and, where different, employing organisation must ensure that the Authentication Token provided to a user is appropriate for that user’s role.

7. GPG 45 outlines four levels of identity assurance. Authentication Tokens will support these four levels of identity assurance. In practice Authentication Tokens will combine the level 3 and level 4 identity requirements. Level 4 being a level 3 identity with the addition of a biometric indicator. A level 3 or level 4 identity is required in order to access clinical, sensitive and person identifiable information. Level 1 and 2 identities will be able to be registered but are aimed at people who do not need access to the types of information that requires a level 3 or 4 identity.

8. Users must be able to easily access support and report and receive assistance with any operational issues, thefts, losses or unauthorised uses of Authentication Tokens, requirements for PIN/password resets, and terminations of Authentication Tokens.

4 Roles & Responsibilities

In order to discharge the responsibilities delegated from NHS Digital in relation to Registration Authority activity there are requirements each organisation which is acting as a Registration Authority must meet in relation to roles and responsibilities within the local organisation. These are as follows:

1. The Board/EMT person accountable for RA activity within the organisation must be overtly identified and named. Part of this ensures that the RA Manager knows who to raise issues with.
2. The Board/EMT individual must report to the Board/EMT annually on RA activity and must sign off on RA Data Security and Protection Toolkit submissions.

3. The RA Manager is responsible for running the governance of RA in the organisation. As such they must agree and sign off on local operational processes and guidance and should assure themselves regularly that these processes are being adhered to (NOTE: local processes must comply with this national policy process and guidance set out by NHS Digital). They are also responsible for registering RA staff in their own organisations and any RA Managers in child organisations. They are also responsible for ensuring the effective training of RA Agents and Sponsors within their organisation.

4. New roles have been created in the Registration Authority software, Care Identity Services, to allow the RA Manager to delegate certain aspects of RA activity. These include Advanced RA Agents, RA Agents (ID checking only) and Local Smartcard Administrators. However, these delegated permissions do not extend to any of the areas covered in point 3 above. This is explained in the following table.

<table>
<thead>
<tr>
<th>RA Manager CANNOT delegate</th>
<th>RA Manager CAN delegate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Responsibility for running RA Governance in their organisation</td>
<td>• Creation of local processes that meet the Registration Authority Policy and guidance for the creation of digital identities, production of NHS Digital smartcards, allocation of other approved devices assignment of access rights, modifications to access and people and certificate renewal and card unlocking</td>
</tr>
<tr>
<td>• Responsibility for ensuring local processes are in place that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and unlocking</td>
<td>• Operation of core RA processes of registering a user, the approval and granting of access, the modification of personal details and the modification of access rights</td>
</tr>
<tr>
<td>• Assignment of RA Agents and sponsors and the registration of RA Agents and Sponsors</td>
<td>• The implementation of the local auditing process</td>
</tr>
<tr>
<td>• Training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process</td>
<td>• Ensuring users accept terms &amp; conditions of Smartcard use when registering them</td>
</tr>
<tr>
<td>• The training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process. A RA Hosting organisation parenting another RA Hosting organisation is responsible in providing training to the RA Manager in the next level down</td>
<td>• Operational security of (old) paper-based RA records</td>
</tr>
<tr>
<td>• Facilitation of the process for agreeing the organisation’s access control positions</td>
<td>• Raising service issues as appropriate and through the correct channels</td>
</tr>
</tbody>
</table>
5. Identity checking must be carried out by those holding an RA role – RA Managers and the RA Agent roles.

A full list of RA policy responsibilities for RA Managers, RA Agents and Sponsors is contained at Appendices 1-3 of this document

5 Requirements in relation to Authentication Tokens

NHS Digital will allow Authorised Devices and iPad Devices in addition to centrally issued Virtual Smartcards and Physical Smartcards. These methods will include approved mobiles, approved tablets, approved devices/operating systems and other approved peripherals and authentication methods. These additional authentication methods must meet the National Institute of Systems and Technology (NIST SP800 – 63 Digital Identity Guidelines for a Authentication Assurance Level 3 authentication, available at https://pages.nist.gov/800-63-3/), this describes the cryptographic strength of authentication methods that is required to access sensitive data. In addition Authorised Devices and authentication methods need to meet FIDO 2 standards for how devices utilise the required cryptography (available at https://fidoalliance.org/) and must be accredited by the FIDO alliance. Any Authorised Device or authentication method that meets both of these standards will be acceptable for authenticating to national clinical systems and the choice of device that meets these standards is down to the local organisation. iPad devices must authenticate using the NHS Digital created authentication app which follows the FIDO patterns of cryptographic exchange.

Authentication Tokens enable an individual to access sensitive patient data, and therefore how they are issued and ensuring safe receipt and appropriate use are of vital importance. As a result, the following are mandatory requirements for Registration Authorities and employing organisations making use of RA activity provided by a local Registration Authority:

1. Authentication Tokens issued to anyone holding RA roles (RA Manager, Advanced RA Agent, RA Agent and RA Agent – ID Checking) must be handed over to that individual in a face to face encounter. This is because RA staff have significant powers in relation to the system and they are entrusted with much of the delegated responsibilities from NHS Digital – therefore it is vital that risks are minimised in the process of the Identity Solution getting to or a device being linked to the right person. It is also a Public Key Infrastructure requirement for these reasons.
2. Organisations must assure themselves that they have a robust and secure process in place to ensure that the Authentication Tokens reach all non-RA users for whom they are intended. This is important to avoid individuals potentially gaining access to patient data when they are not the person entitled to do so.

3. Organisations should ensure that their infrastructure is secure, in particular ensuring they meet the Warranted Environment Specification issued by NHS Digital available at https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes

4. Only the user for whom the Authentication Tokens is intended should know their passcode for their Authentication Tokens, no-one else should, including RA staff. If anyone else knows the user’s passcode it breaches the Authentication Tokens terms and conditions of use and the Computer Misuse Act 1990.

5. When Identity Solution users leave an organisation should have their access assignment end dated in that organisation. However, unless it can be reasonably foreseen that they will not require access in another organisation in the future, leavers should retain their Physical Smartcard or Virtual Smartcard if this is stored on their personal mobile phone. Users of other Authorised Devices or iPad Devices will return these devices to their organisation before they leave.

6. It is mandatory that users sign the Terms & Conditions applicable to access to the NHS Care Records Service detailed at https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities. This reminds them of their responsibilities and obligations, including not sharing their Identity Solution, and not disclosing their passcode to others.

7. RA staff (RA Managers, Advanced RA Agents and RA Agents) are reminded that it is their responsibility to ensure that users comply with these terms and conditions.

6 Local RA Policy

It is a mandatory requirement that organisations that are local Registration Authorities and run local RA activity have a local policy outlining their approach. The following are mandatory requirements within the local organisation’s policy.

1. The name of the Board/EMT accountable person and the RA Manager within the organisation must be named within the policy. The policy needs to outline the governance requirements placed upon these individuals. The local organisation’s policy must be updated to reflect any changes to the named individuals.

2. The policy must describe how access rights will be granted and revoked in a timely way, ensuring that requirements for staff to be able to access electronic records in a timely way can be met and that individuals do not retain access within an organisation once they have left that organisation.

3. The policy must not contradict the mandatory requirements contained within this national RA policy document. At a minimum the policy must cover:
   i. Governance arrangements
ii. A demonstration of the adherence to this policy document requirements in relation to the verification of identity
iii. Roles & responsibilities
iv. Authentication Token use

4. The policy must be formally signed off by the organisation at an appropriately senior level, e.g. the EMT, the IG Committee on a delegated authority basis, etc.

7 Failure to comply with policy requirements

Where NHS Digital is notified of significant breaches to this policy, they will consider the situation and take appropriate remedial action. This will include discussing the situation with the organisation but may result in discussions with regulatory or professional bodies depending upon the seriousness of the situation.
Appendix 1 – RA Manager Responsibilities

• RESPONSIBLE for running RA Governance in their organisation – RA Managers CANNOT DELEGATE THIS

• Responsible for the development of local processes that meet policy and guidance for the creation of Authentication Tokens, digital identities, production of smartcards, assignment of security device, assignment of access rights, modifications to access and people, removal of access rights in a timely fashion where there is no business justification for the rights to be retained and certificate renewal and card unlocking

• Implements local RA policy and RA processes adhering to national guidance and this policy

• Assign, sponsor and register RA Agents and Sponsors

• Train RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process – If an RA hosting organisation with a child hosting organisation – need to train RA Manager at next level down

• Facilitate the process for agreeing the organisations access control positions

• Responsible for auditing

• Responsible for ensuring users are compliant with the terms and conditions of Smartcard usage and other registered devices

• Verifies user’s ID to GPG45 Level 3 or 4, when they register users

• Ensuring leavers from an organisation have their access rights removed in a timely way

• Responsible for the security of (old) paper-based RA records

• Ensure all service issues are raised appropriately locally and nationally
Appendix 2 – RA Agent Responsibilities

- Verify users ID to GPG45 Level 3 or 4
- Register users and provide them with Authentication Tokens
- Grant users access assignment
- Renew Smartcard certificates for users if self-service functionality not used
- Responsible for ensuring users at the time of registration or assigned a role in the organisation comply with the individual terms and conditions applicable to access to the NHS Care Records Service Ensuring leavers from an organisation have their access rights removed in a timely way
- Adhere to local processes that meet policy and guidance for the creation of Authentication Tokens, digital identities, production of smartcards, allocation and registration of other approved devices, assignment of access rights, modifications to access and people and certificate renewal and card unlocking
Appendix 3 – Sponsor Responsibilities

• Can raise requests for new users
• Approve users assignment to access control positions, or,
• Directly assign users under position management
• Unlock Authentication Tokens and renew certificates for non-RA staff
• DO NOT verify users ID