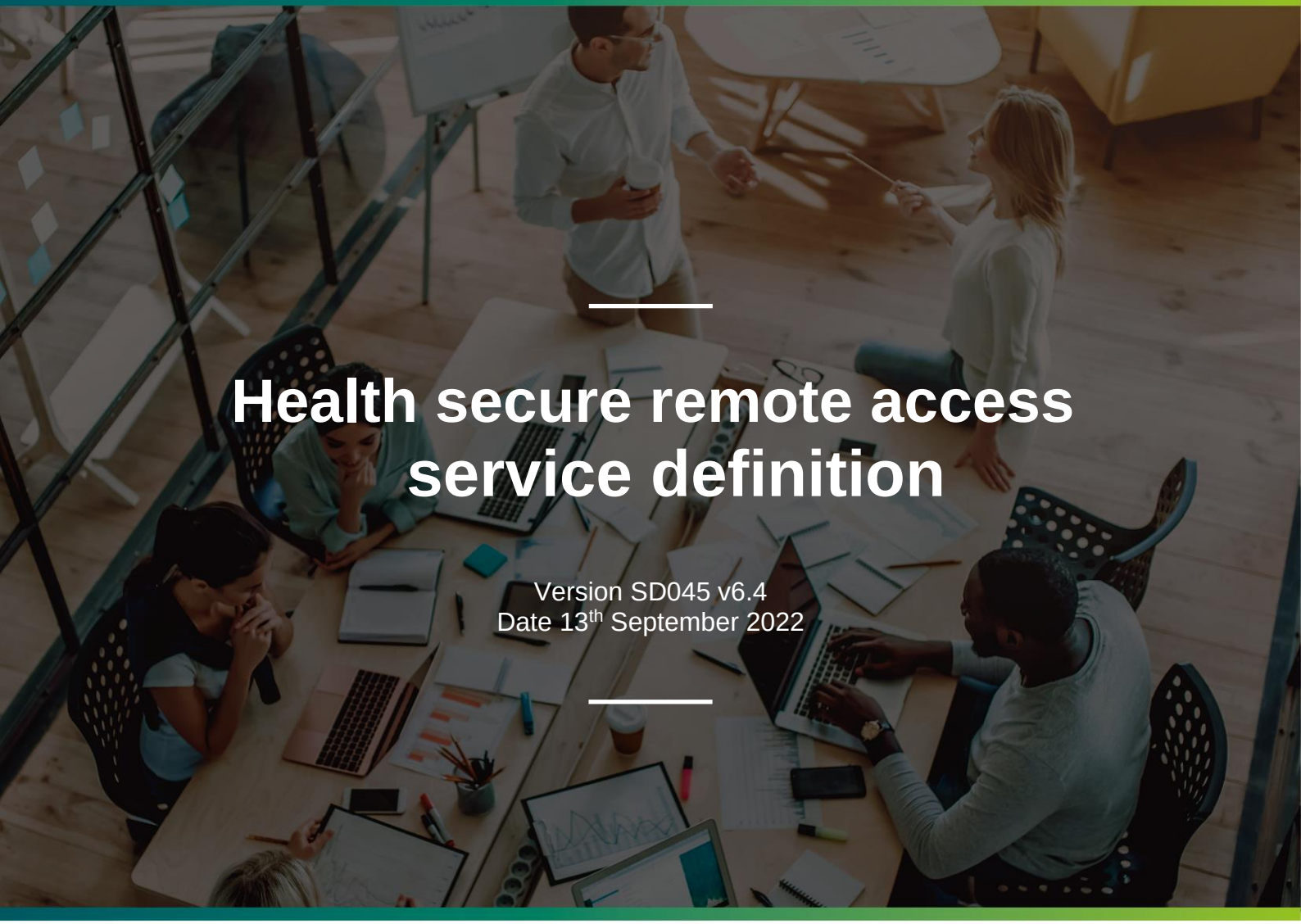


Health secure remote access service definition

Version SD045 v6.4
Date 13th September 2022

redcentric

AGILE • AVAILABLE • ASSURED

1. Service overview

1.1 Service overview

Redcentric's Healthcare Secure Remote Access Service offers a robust, flexible, and secure way for healthcare professionals to access technology applications offered by the National Health Service (NHS) whilst away from their usual work location.

Redcentric's Healthcare Secure Remote Access Service is NHS approved and offers field-based Health workers the opportunity to take advantage of new approaches to healthcare designed to help reduce overhead expenditures, facilitates data exchange and enhances Customers' experience.

A piece of software on the user's PC, tablet or other remote device communicates with the resilient Redcentric platform across a ubiquitous Internet connection and a secure tunnel is built between the two. The user's data is passed through this tunnel, then from the secure remote access platform through Redcentric's resilient HSCN gateway to access healthcare applications and resources. The Healthcare Secure Remote Access Service includes highly secure two-factor authentication to ensure that only legitimate users can connect. Strong encryption is implemented on the tunnel between the user and the platform to protect sensitive information in transit.

1.2 Benefits

- Facilitates remote working. Enables frontline healthcare staff to access key resources remotely, supporting such services as Tele-health, community care nursing and out of hour's GP
- Supports business continuity. Allows users to continue working away from their formally connected offices, enabling business continuity and recovery from disastrous events
- Increased front-end focus. Allows Customers to concentrate on their core business activities
- Scalable and flexible. Delivers best-of-breed remote access connectivity and can scale easily to meet the needs of Customers large and small
- Access to value-adding service propositions. Designed to support and enhance the entire Redcentric portfolio of cloud-based services

2. Service description

2.1 Remote access solution

A small piece of software is deployed on the end-user's Lap-top (or similar). With suitable Internet access (possibly Wi-Fi or mobile Internet connection), and when initiated by the user, the software builds a secure communication tunnel across the Internet to Redcentric's remote access platform. The end user identifies them self to the platform using a supplied software authentication token which can run on a laptop, Mac or smartphone (or optional hardware fob). This user authentication is dependent on two factors; something the user knows and something the user has. When prompted for authentication, the user inputs a pin-code they have memorized plus the output from the token. This robust, secure authentication, in conjunction with the encryption applied to the data tunnel provides the security to meet current NHS Security requirements.

2.2 Basic operation

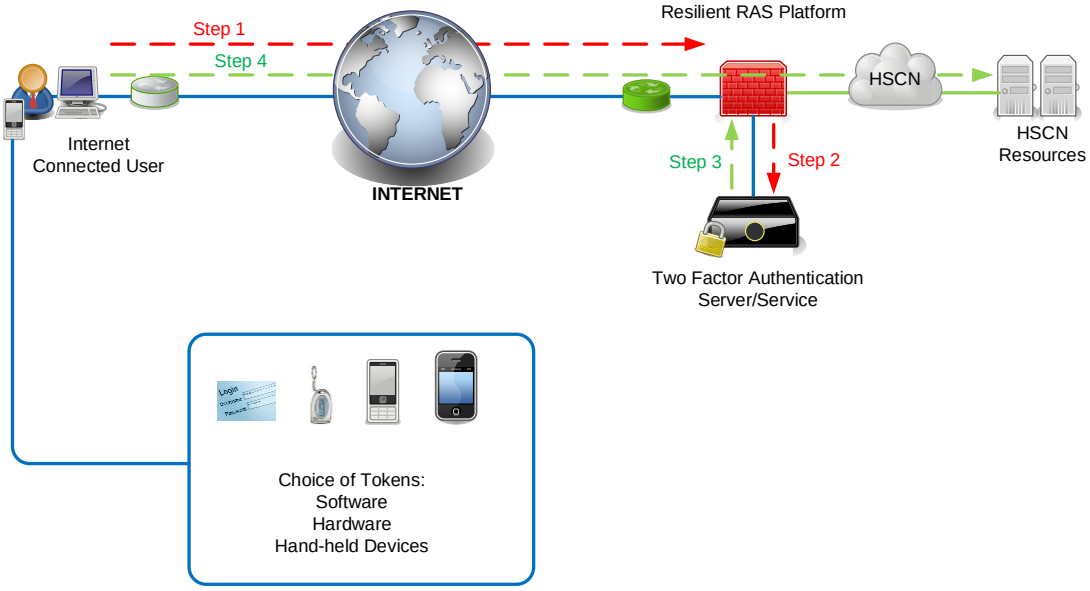
The steps shown in the diagram below illustrate how users are connected to healthcare resources from a remote location:

Step 1: The user establishes a connection to the platform using preconfigured client software which is loaded on their end device. During negotiation, the user presents their username and authentication credentials i.e., Factor-1 - Their PIN and Factor-2 - The output from their token (also supplied)

Step 2: The remote access platform sends the user's credentials to the two-factor authentication platform

Step 3: The authentication platform validates the user's credentials

Step 4: Assuming the user is authenticated, the encrypted tunnel is built, and the user is provided access to the HSCN network and its resources



2.3 VPN Client Software

Most modern Operating Systems on laptops and other mobile devices include a suitable VPN client. However, Redcentric also supplies a client that can be used on a wide variety of devices and operating systems including Microsoft Windows and Apple Mac OS X.

2.4 Authentication token types

Redcentric offers both software and hardware tokens.

Software tokens can be deployed on tablets, laptops and smart-phones. Software tokens reduce the cost of ownership as they are easier to deploy and can be re-issued to an alternative device as required.

The hardware token option can be used when no lap-top, tablet or smart-phone is available. Its low weight and size make it ideal for use on a key-ring but consideration needs to be made to battery-life and the greater potential for loss, damage and increased likelihood of losing synchronisation.

Redcentric supports software tokens on the following Operating System platforms:

- Apple iOS
- Blackberry
- Android
- Windows phone
- Mac OS
- Windows desktop

2.5 Mixing, changing and issuing multiple tokens

It is possible to order a combination of software and hardware tokens across a group of users. For example, it is possible to deploy software tokens on laptops of 30% of users, software tokens on smartphones of 60% of users and issue the remaining 10% of users with hardware tokens.

It is not possible to swap between software and hardware tokens during the term of the contract.

A single user can be issued with more than one token, but this has a charging implication as the service charge is based on the number of token licenses on the system, not the number of users.

2.6 Customer dependencies

The Customer is responsible for:

- Contacting their HSCN software/application supplier(s) and arranging for traffic to/from remote access IP-addresses (supplied by Redcentric after installation) to be allowed.
- Distribution, set-up, and support of remote VPN software to individual users
- Identifying and sourcing suitable VPN software for device / operating systems combinations not supported on the supplied software
- Adding user details to the platform, and allocating each user a token licence
- Triggering the software token allocation for each user or physically allocating hardware tokens to users
- Undertaking user support and administration using the Administration Portal (e.g., user password re-set)
- Returning faulty hardware tokens to Redcentric (in batches)
- Making provision for suitable Internet connectivity for end users
- Timely ordering and distribution of replacement hardware tokens when the internal battery reaches end-of-life

2.7 Redcentric responsibilities

As part of the Healthcare Secure Remote Access Service, Redcentric performs the following functions:

- Configures the Customer environment on the remote access and authentication platforms
- Loads token licences onto the platform
- Provides the Customer with a link to VPN client software
- Despatches hardware authentication tokens to a single Customer location usually in a single shipment
- Configures the platform to access the HSCN network
- Notifies customer of the IP-address range(s) used for remote access, so that they can be supplied to Software/application suppliers
- Maintains the resilient centralised authentication and remote access platforms

2.8 Ordering and service set-up

Under normal circumstances, initial and additional user licences would take no more than 15 working days to commission on the platform.

2.9 Replacement of authentication fobs

Redcentric will replace hardware tokens that develop a fault at no charge during the term of the contract.

Customers with a large estate of hardware tokens are advised to order extra units in-advance, to replace tokens that become lost or damaged.

Customers are required to order hardware tokens to replace those where the battery reaches the end of its useful life (typically four years or more).

Software tokens cannot be lost, damaged or become faulty; they can be re-issued, as required, via the administration portal.

2.10 Administration portal

As part of the Healthcare Secure Remote Access Service, Redcentric provides access to an administration portal. The Customer's help desk staff use the portal to provide support to end users according to the Customer's internal service levels for straight-forward tasks, e.g., soft token re-issue and user password re-sets.

One token/licence is required for each of the Customer's administrators. To enforce security, administrators are required to use the system to log on to the administration portal.

2.11 LDAP agent

Optionally, a Lightweight Directory Access Protocol (LDAP) synchronization agent is available for Customers to deploy in their environment. Once installed, the agent monitors LDAP groups for membership changes and updates user information on the authentication platform to reflect these changes. The agent reads only basic information from the directory and communication from the agent to the authentication platform uses strong encryption. Specific details of the LDAP agent, including the directories that can be supported, is available on request. LDAP agent set-up and support incurs additional charges.

2.12 Monitoring

Redcentric monitors the remote access platform for availability and performance against pre-determined criteria. Redcentric periodically sends an authentication request from a remote device to the authentication platform to ensure that the platform is operating correctly and returning authentication responses. Response time-out, authentication failure of test polls and platform issues automatically trigger the creation of a fault ticket, and the issue is subsequently investigated by a Redcentric engineer.

2.13 Support

Redcentric staff support the platform, the administration portal and provide system wide support to the Customer's help desk staff. Redcentric do not offer support directly to end users.

2.14 Documentation and training

Redcentric will provide a user guide and an administrator's guide. In addition, Redcentric will provide telephone support as the Customer adds the first few users to the system via the administration portal.

2.15 Reporting

An extensive selection of reports can be accessed from the Authentication Administration Portal including, for example authentication history, token counts & inactive users. No reporting information is available regarding the amounts of data transferred.

2.16 Simultaneous use, contention and fair use policy

The platform has been designed to meet the Service Levels set out in section 4 under standard operating conditions. The Healthcare Secure Remote Access Service has been built to meet most Customers' needs and to make it cost effective, the platform is built on the basis that only a fraction of potential users will connect at any one time. In the event that a Customer persistently consumes a disproportionate amount of capacity, to the detriment of other Customers, that Customer may have limits applied to the resource they can consume including a limit on their maximum number of simultaneous connections.

2.17 Hardware ownership

Redcentric remains the owner of hardware tokens until the Healthcare Secure Remote Access Service terminates, when ownership of hardware tokens is transferred to the Customer. The Customer is required to dispose of hardware tokens in accordance with Waste Electrical and Electronic Equipment recycling (WEEE) regulations or return them to Redcentric in a single batch for disposal when the 2FA Service terminates.

3. Implementation and acceptance

3.1 Acceptance criteria

The following are the Acceptance Criteria applicable to the Healthcare Secure Remote Access Service:

- Delivery of hardware tokens to Customer
- User guide supplied to Customer
- Administrator guide supplied to Customer
- Supply of client software to Customer
- One Customer administrator account set-up on the administration portal
- Customer administrator can access portal and confirms licences are in the resource pool
- Token allocation and user set-up for at least one end user – with support from Redcentric if required
- Supply SRAS IP-address range(s) to the Customer so that application access can be arranged
- Test to confirm that end user can connect to the platform and access healthcare resources where permission has been granted

4. Service levels and service credits

4.1 Service levels

The Service Level applicable to the Healthcare Secure Remote Access Service is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level	Not less than 99.5%

4.2 Exclusions from availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- An extreme volume of users connecting to the platform as a result of an event that is beyond the control of the parties
- Any failure of HSCN connectivity or services

4.3 Floor service level

The Floor Service Level applicable to the Healthcare Secure Remote Access Service in respect of Availability shall be 85% in any given Month.

4.4 Service credits

The Service Credits applicable to the Healthcare Secure Remote Access Service shall be calculated as follows:

In the following table:
"≥" means "greater than or equal to"
"<" means "less than"
"MS" means the total Charges payable in respect of the Healthcare Secure Remote Access Service for the same Month

Service Availability	Service Credit
≥99.5%	none
≥99.0% but <99.5%	5% of MS
≥97.0% but <99.0%	15% of MS
<97.0%	20% of MS

5. Data processing

5.1 Data processing scope

- The Healthcare Secure Remote Access Service facilitates secure transport of IP packets between remote workers and the HSCN healthcare network.
- The Healthcare Secure Remote Access Service does not involve any storage or backing up of data.

5.2 Data storage and encryption

- Industry standard encryption protocols are used to help keep traffic traversing the Internet private.
- Redcentric does not capture, inspect, analyse, store or share the traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the Customer's traffic in order to investigate and diagnose a very specific problem, e.g., to help resolve a problem relating to IP packet corruption. Such diagnosis would involve the examination of a small sample of IP packets.

5.3 Data processing decisions

- Redcentric does not make any data processing decisions in relation to the Healthcare Secure Remote Access Service. Any processing of data over the systems when using the Healthcare Secure Remote Access Service for transit is instigated, configured, and managed by the Customer and/or NHS-Digital.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Healthcare Secure Remote Access Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4 Sub-processors

- Data traverses the public Internet between the remote user and the Healthcare Secure Remote Access platform gateway. Redcentric uses multiple upstream tier-1 Internet Service Providers (eg. Cogent, Level-3 and LINX etc.) for Internet connectivity. Redcentric has no control of traffic that traverses the Internet with regards integrity, confidentiality and/or reliability. Consequently, the Healthcare Secure Remote Access platform makes use of user authentication and data encryption to help maintain data confidentiality and integrity.
- Data to/from the remote user traverses Redcentric's HSCN gateway connections to the HSCN network; this is supplied by NHS-Digital.
- Redcentric currently uses a product from third party company, Gemalto, to implement multi-factor user authentication. Gemalto hold basic credentials of remote users only. Gemalto does not have access to Customer data that passes between the remote user and the healthcare network.
- No other third parties are involved in delivering the Healthcare Secure Remote Access Service, and there are no sub-processors appointed by Redcentric.

5.5 Customer access to data

- The Customer control its own platforms which use the Healthcare Secure Remote Access Service to carry data, and the Customer therefore has full access to its own data.

5.6 Security arrangements and options

- The core Infrastructure delivering the Healthcare Secure Remote Access Service is hosted at both Redcentric and third-party locations. All locations meet physical security standard ISO27002 section 11.1 or equivalent.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED