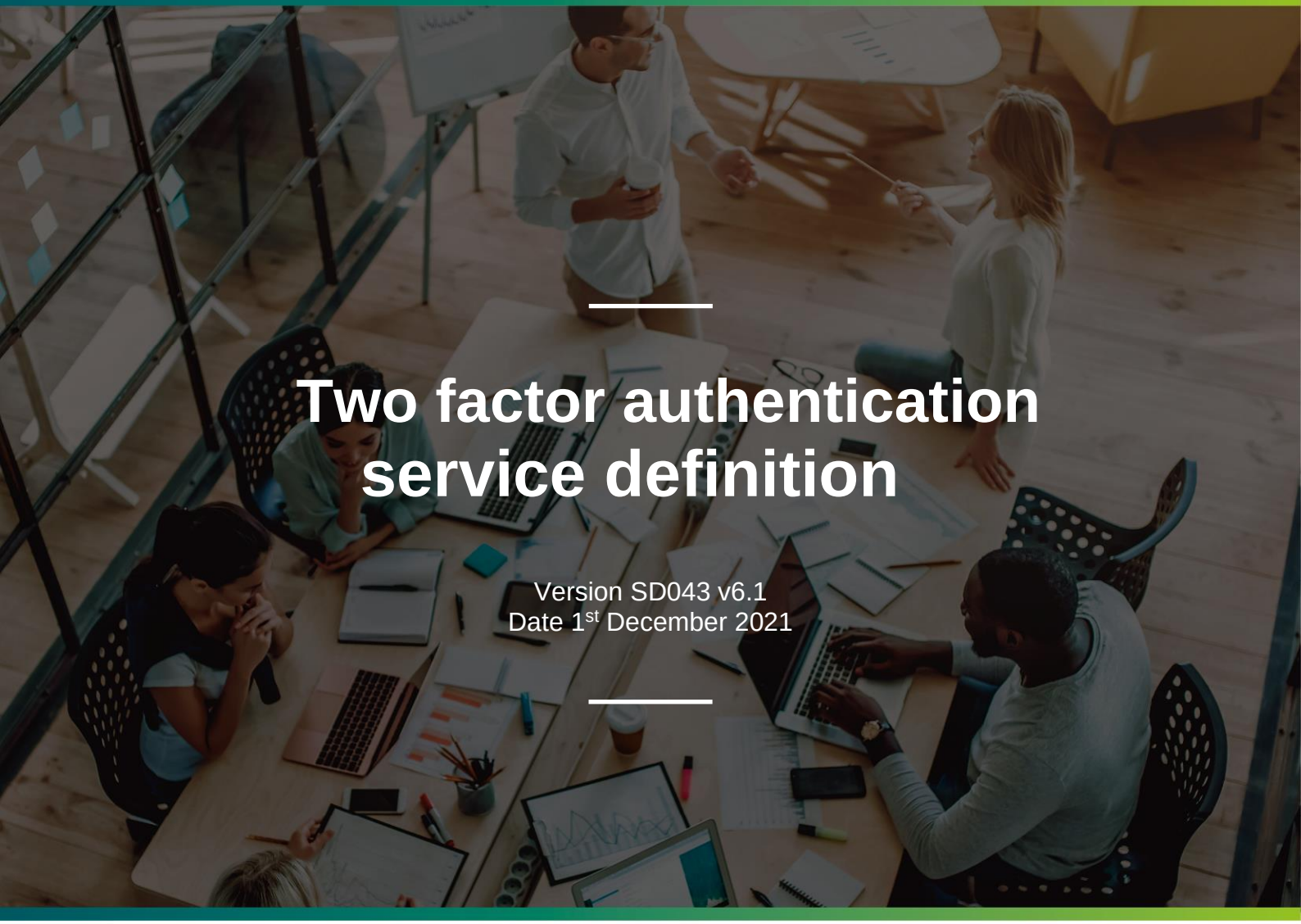

Two factor authentication service definition

Version SD043 v6.1
Date 1st December 2021

redcentric

AGILE • AVAILABLE • ASSURED

1. Service overview

1.1 Service overview

Redcentric's 2-factor Authentication (2FA) Service offers a robust, flexible and secure way to authenticate user connections requests to network devices. The 2FA Service can be deployed on both Customer managed and Redcentric managed network devices. The 2FA Service offers a far more secure and scalable alternative to static passwords.

1.2 Benefits

- More secure than static or rotating passwords
- Low per-token, per month charge
- Highly scalable
- Choice of hardware or software tokens
- Highly resilient authentication platform
- Fast, easy provisioning
- Easy to use administration portal
- Integrates with other Redcentric services

2. Service description

2.1 Multifactor authentication

Static passwords are notoriously vulnerable to sustained guess attempts, and it is generally accepted that multiple factor authentication provides a significantly more secure authentication mechanism. With the Redcentric 2FA Service, authentication is based on something the user knows and something the user has. When prompted for authentication, the user inputs a pin-code they have memorised, i.e. something they know, plus the output from a 'token', something they have. The output of the token changes each time it is used making repeated guesses virtually pointless.

2.2 Authentication of network devices

Redcentric's 2FA Service is designed to provide robust authentication for network devices. Customers can configure their own network devices to off-load authentication requests to the Redcentric authentication platform. Alternatively Customers subscribing to Redcentric's Managed Firewall Service can enhance security of access attempts by subscribing to the optional 2FA Service. The 2FA Service makes use of the Remote Authentication Dial-in User Service (RADIUS) protocol for communication between network devices and the authentication platform. One common use of the 2FA Service is to provide strong authentication of remote users wishing to connect to the corporate firewall using IP-sec or similar security tunnel protocols. Subject to appropriate design, it may be possible to use the 2FA Service for other applications.

2.3 Associated and complimentary services

For Customers that do not have the in-house skills or the inclination to design and manage firewall devices, Redcentric offers a Managed Firewall Service. Please see the Managed Firewall Service Definition for details.

Customers with large, changing or complex requirements to support remote workforces can subscribe to Redcentric's Secure Remote Access Service (SRAS). SRAS delivers all of the required components (central tunnel termination, central Internet access bandwidth, client software and 2FA) to provide an 'all-in-one' remote access solution.

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 Customer dependencies

The Customer is responsible for:

- Adding user's details to the platform and allocating each user a token licence
- Triggering software token allocation for each user or physical allocation of 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)
- The centralised authentication platform is accessed via the Internet so appropriately configured Internet access needs to be available at network devices that defer authentication requests to the platform.
- Timely ordering and distribution of replacement hardware tokens when the internal battery reaches end-of-life

2.6 Redcentric responsibilities

As part of the 2FA Service, Redcentric performs the following functions:

- Configure Customer environment on the platform
- Load token licences onto the platform
- Despatch hardware tokens to a single Customer location, usually in a single shipment
- Configure the platform to accept authentication requests from specific network devices
- Maintain the resilient centralised authentication platform.

2.7 Ordering and service set-up

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

2.8 Replacement 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.

2.9 Administration portal

As part of the 2FA 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 2FA token/licence is required for each of the Customer's administrators. To enforce security, administrators are required to use the 2FA system to log on to the administration portal.

2.10 LDAP agent

A Lightweight Directory Access Protocol (LDAP) synchronization agent is available for Customers to deploy in their environment. Once installed, the LDAP synchronization 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.

2.11 Monitoring

Redcentric periodically sends an authentication request from a remote device to the platform to ensure that the platform is operating correctly and returning authentication responses. Response time-out or authentication

failure automatically triggers the creation of a fault ticket, and the issue is subsequently investigated by a Redcentric engineer.

2.12 Support

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

2.13 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.

2.14 Reporting

An extensive selection of reports can be accessed from the administration portal including, for example, authentication history, token counts & inactive users.

2.15 Hardware ownership

Redcentric remains the owner of hardware tokens until the 2FA 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 2FA Service:

- Delivery of hardware tokens to Customer
- User guide supplied to Customer
- Administrator guide supplied to Customer
- One Customer administrator account set-up on 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
- Test to confirm that 2FA Service authenticates the network device(s)

4. Service levels and service credits

4.1 Service levels

The Service Level applicable to the 2FA Service is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level	Not less than 99.99%

4.2 Floor service level

The Floor Service Level applicable to the 2FA Service in respect of Availability shall be 85% in any given Month.

4.3 Service credits

The Service Credits applicable to the 2FA 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 2FA Service for the same Month

Service Availability	Service Credit
≥99.99%	none
≥99.0% but <99.99%	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 2FA Service provides electronic system user authentication
- The 2FA Service does not involve any storage or backing up of data beyond basic user credentials including email address and name etc.

5.2 Data storage

- Redcentric does not capture, inspect, analyse, store or share the Customer's traffic/data.
- Redcentric's sub-processor, Gemalto (see section 5.4) below) holds certain traffic/data.

5.3 Data processing decisions

- Redcentric does not make any data processing decisions in relation to the 2FA Service. Any processing of data over Customer systems when using the 2FA Service is instigated, configured and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the 2FA 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

- Redcentric uses a product from third party company, Gemalto, to implement multi-factor user authentication. Gemalto hold basic credentials of remote users only. Otherwise, Gemalto does not have access to Customer data.
- No other third parties are involved in delivering the 2FA Service, and other than Gemalto there are no sub-processors appointed by Redcentric.

5.5 Customer access to data

- The Customer controls its own platforms which use the 2FA Service for authentication, and the Customer therefore has full access to its own data on those platforms.

5.6 Security arrangements and options

- The core Infrastructure delivering the 2FA 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