InTechnology Plc

N3 Secure Remote Access

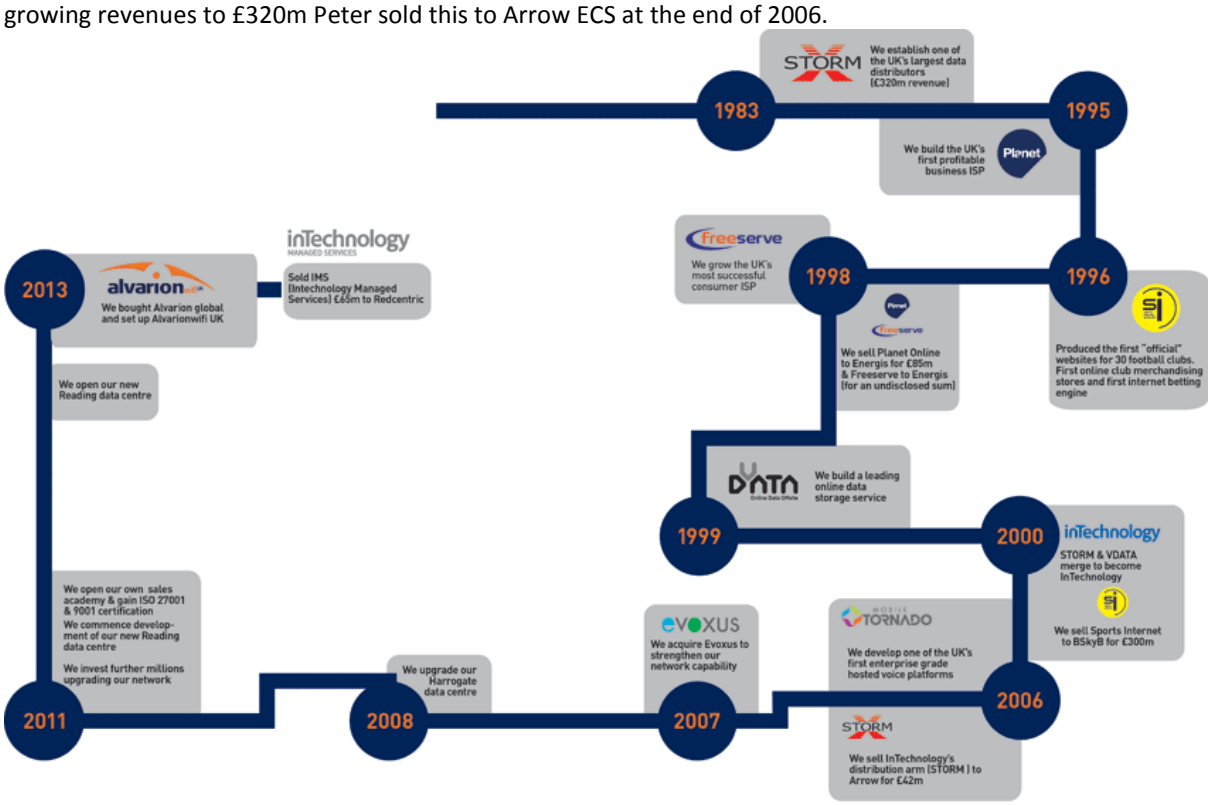
Service Definition
G-Cloud edition

intechnologyplc

Public

InTechnology Plc overview

In 2013, Intechnology plc entered its fourth decade at the forefront of the IT industry in the UK, it all began in 1983 from a small office in Wetherby where Peter Wilkinson the founder and owner started the first Storage Only solutions distribution business which grew over a period of time to be the UK's largest. Impressively growing revenues to £320m Peter sold this to Arrow ECS at the end of 2006.



With his interest in communications and networks in 1995 Peter started the first business only internet service provider "Planet Online".

In 1998 "Planet Online" was the largest UK business ISP which was sold to Energis in the same year.

During 1998 Peter invented the business model to provide free internet access to home users in the UK. In order to bring this to the mass market Peter partnered with Dixon Stores group to launch under the brand of "Freeserve" the UK's most successful domestic internet service provider.

During the period of Planet Online Peter became extremely interested in the provision of content realising that connectivity was becoming a commodity. He founded Planet Football and became the official provider of football club websites to over 25 clubs in the old first and second divisions.

Peter reversed Planet Football into the AIM listed Sports Internet group and continued to find revenue streams for the huge traffic that the football club websites were attracting. Peter acquired Opta statistics to provide analytics to the fans and then purchased Surrey Sports (a betting company). This enabled Sports Internet to be the first company in the UK to provide online betting on football matches on the internet.

This business was sold to BSkyB in 2000 and became Skybet.

In 2000 Peter reversed his Storm business into the AIM listed InTechnology PLC and also started InTechnology Managed Services. This became one of the most respected and largest Infrastructure managed services businesses in the UK. This was sold to Redcentric in November 2013.

In 2006 Peter took a stake in the leading PTT (push to talk) technology business "Mobile Tornado". The technology is so impressive and has so many different applications including security camera technology and the communication protocol that really is superior to the standard PMR devices InTechnology plc took a further stake in the business.

InTechnology plc has also developed a voice recording solution which trades under the Live-PA brand, InTechnology also passionately believes that Digital Healthcare is vital to the future of both the NHS and its patients and to this end under it's brand "Inhealthcare" InTechnology has developed the first accredited patient platform in the cloud along with a number of clinical pathways, enabling patients to monitor their conditions from home.

With the rapid development and uptake of mobile devices and tablets the lack of good WiFi has left a huge hole in the marketplace. Having spent years searching for a technically advanced WiFi manufacturer Peter eventually found and bought "Alvarion" in November 2013. Once he'd acquired this business he saw a huge market opportunity in the UK for Smart Cities, Stadiums, Arenas, Greenfield events etc. which wasn't being fulfilled by the predominantly US WiFi manufacturers or any of the large UK telecom providers.

In January 2014 InTechnology Plc launched InTechnology Wi-Fi Ltd where it will use its previous models and expertise to deliver content rich Wi-Fi solutions to cities, stadiums, arenas and greenfield sites.

An overview of the G-Cloud Service (functional, non functional);

Non functional

InTechnology's **N3 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.

InTechnology's N3 Secure Remote Access Service is HSCIC / 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 enhance customers' experience.

A piece of software on the user's PC (or tablet or other remote device) communicates with the resilient InTechnology platform and a secure tunnel is built across the Internet connection to this platform. The user's data is passed through this tunnel, then through InTechnology's resilient N3 gateway to access N3 resources. The 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.

Benefits

- **Enables 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 consultancy.

- **Supports business continuity**

The service allows users to continue working away from their formally connected offices, enabling business continuity and recovery from disastrous events.

- **Increased front-end focus**

InTechnology's N3 Secure Remote Access Service allows customers to concentrate on their core business activities.

- **Scalable and flexible**

The service 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**

The service is designed to support and enhance the entire InTechnology portfolio of cloud based services.

Summary

- Access to valuable healthcare information out of the office
- Low per-user monthly charge
- Highly scalable
- Choice of Hardware or software authentication tokens
- *User database can be synchronised with Customer's LDAP database*
- *Fast, easy provisioning*
- Easy to use administration portal
- Health and Social Care approved solution
- InTechnology's N3 Secure Remote Access Service is private and secure, enabling IP connectivity to various company locations, the N3 spine, suppliers and 'extranets'.

Functional

Remote Access Solution

A small piece of software is deployed on the end-user's Lap-top (or similar). With suitable Internet access (possibly wifi or a 3G mobile connection), and when initiated by the user, the software builds a secure 'tunnel' across the Internet to InTechnology's remote access platform. The end user identifies themselves to the platform using a supplied hardware key-fob token (or software version that can be run on many smart-phones). 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 NHS Security requirements.

Basic Operation

The steps shown in the diagram below illustrate how users are connected to N3 resources from a remote location:

Step 1: The user establishes a connection to the platform using suitable IP-sec compliant VPN client software. During negotiation, the user presents their username and authentication credentials i.e.

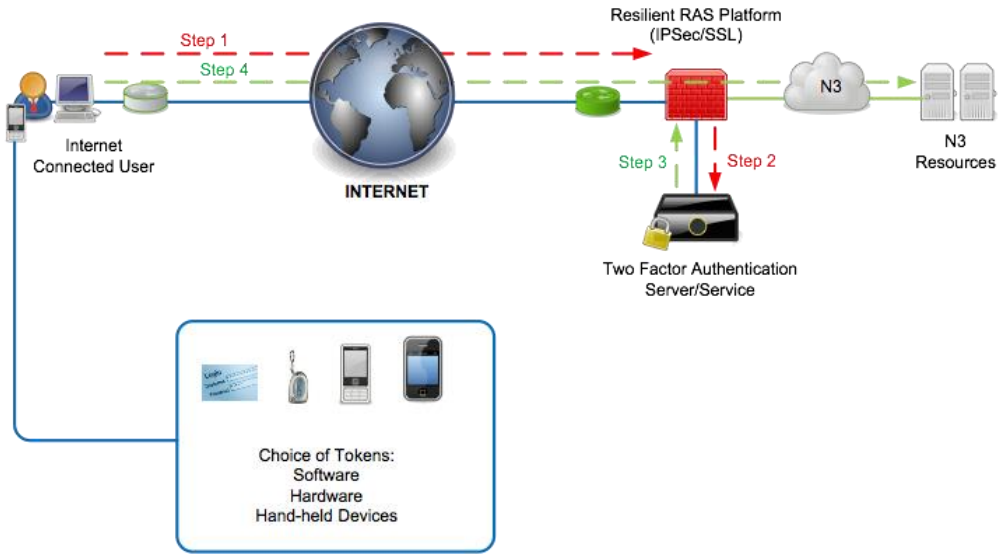
Factor-1 - Their PIN

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 N3 network and its resources



VPN Client Software

InTechnology will supply an IP-sec compliant client that can be installed on the following Microsoft© Windows© Operating Systems:

- Windows 7 on x64 (64-bit)
- Windows 7 on x86 (32-bit) only
- Windows Vista on both x86 (32-bit) and x64
- Windows XP on x86

InTechnology may offer an alternative client from time-to-time and any such client may be supported on different Operating Systems, as they evolve.

Customers with users wishing to use mobile devices with other Operating Systems are free to source, deploy & support alternative IP-Sec compliant clients but InTechnology cannot offer compatibility assurances.

Authentication Token Types

InTechnology offers both Hardware and Software authentication tokens.

The hardware token is an extremely robust device, having a steel outer shell. Its low weight and size make it ideal for use on a key-ring or similar.

Software tokens can be deployed on both traditional laptops and also on smart-devices. Software tokens reduce the cost of ownership as they are easier to deploy and less likely to be lost.

InTechnology supports software tokens on the following Operating System platforms:

Smart phone tokens

- phone iOS 4.1+
- Blackberry

- Android 2.2

Software Tokens - Windows PCs (32/64 bit)

- XP
- Vista
- Windows 7
- 2003 Server Family
- 2008 Server Family

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 smart-phones 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. The service charge is based on the number of token licenses on the system, not the number of users so it would double the cost of the service to provide each user two tokens.

Responsibilities

As part of the Service, InTechnology performs the following functions:

- Configures the customer environment on the remote access and authentication platforms
- Loads token licenses onto the platform
- Provides the customer with sample VPN client software
- Dispatches hardware authentication tokens to a single customer location usually in a single shipment
- Configures the platform to access N3 resources as per the pre-sale design
- Maintains the resilient centralised authentication and remote access platforms

The customer is required to perform all other functions including, but not limited to:

- Distribution , set-up and support of remote VPN software to individual users
- Identifying and sourcing suitable IP-sec compliant client software for device / operating systems combinations not supported on the supplied software
- Adding user details to the platform, and allocating each user a token license
- Trigger the software token allocation for each user or physically allocate hardware tokens to users

- Undertake user support and administration using the Administration Portal (eg. user password re-set)
- Return faulty hardware tokens to InTechnology (in batches)
- Make provision for suitable Internet connectivity for end users

Pre-Requisites

The Service does not include any form of Internet access for remote users, it is essential that suitable Internet access is made available (for example using a 3G mobile SIM).

Access to N3 resource is approved and granted by HSCIC; the usual application and approval process need to be made for these services.

Information Assurance

Business Impact Level / Government Security Classifications for protected assets

- InTechnology's Data Centre Services and supporting operations have been approved to the BIL4,4,4 "Confidential" standard.
- Advent-IM are our chosen CESG Government approved assurance partners for BIL & Government protected assets and services
- InTechnology are progressing "PSN" certification for all appropriate services. All services will be certified using the relevant Government security classifications (BIL / O,S,TS), to be completed within calendar year 2014.

Supporting Certifications

The below formal certifications demonstrate the capability and alignment with Information Assurance requirements as mandated by the Public Sector.

- ISO27001 Certified – all Business areas, Harrogate & Reading locations.
- ISO9001 Certified – all Business areas, Harrogate & Reading locations.
- Authorised to transmit, process and store Person Identifiable Data (PID)
- HSCIC IGSoC-compliant commercial third party
- HSCIC accredited and compliant data centre hosting facilities, including for Clinical Systems environments

Government Security Classifications

InTechnology N3 Secure Remote Access Services do not store data; they offer high performance, cost effective to the HSCIC Healthcare N3 network

Advent-IM are our chosen CESG Government approved assurance partners for protected assets and services

InTechnology are progressing "**PGA**" certification for all services, to be completed within calendar year 2014.

Connection Code and Practise

The Connection Code and Practice for partners and customers using N3 Secure Remote Access Services into the Health and Social Care Healthcare Network has been designed to assist the implementation of healthcare projects and is based in part upon elements of ISO27001:2005 and N3's Acceptable Use Policy. All NHS and

non-NHS organisations are required to sign up to the policy documents making up the Code of Connection before N3 Secure Remote Access Services can be provisioned.

On-boarding processes/scope

Connection Code and Practice

The Connection Code and Practice for partners and customers using N3 Secure Remote Access Services into the Health and Social Care Healthcare Network has been designed to assist the implementation of healthcare projects and is based in part upon elements of ISO27002:2005 and N3's Acceptable Use Policy. All NHS and non-NHS organisations are required to sign up to the policy documents making up the Code of Connection.

Change Requests

The majority of customer change requests for the N3 service are dependent upon changes, approvals or authorisation by NHS H&SC and/or BTSP (The N3 core infrastructure supplier). InTechnology's target for undertaking changes requests reflects these supplier commitments and is currently 10 working days.

Lead times

The initial order for the service follows InTechnology's standard order process. Subsequent orders for additional users will also follow the standard process however InTechnology anticipates enhancing the on-line Services Portal to include orders for additional users.

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

On-Boarding Process

InTechnology support the process of migration from an existing N3 service provider in addition to greenfield deployments, InTechnology's design consultants will work with you on building a transition plan that will include all end-end solution design and design management, for example migration of Access Control Rules, IP addressing, Domain Name Server information and logical security tier configuration. In addition InTechnology's consultants will ensure that absolute Information Governance is maintained by working with you through all HSCIC information governance documentation.

Administration Portal

As part of the Service, InTechnology provides access to an administration portal. The customer's help desk staff use the portal for initial user set-up and can use it to provide support to end users according to the company's internal SLA for straight-forward tasks, like user password re-sets.

LDAP Agent

An 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.

Replacement Authentication Fobs

InTechnology will replace Faulty hardware authentication tokens at no charge during the term of the contract.

Hardware tokens can be purchased to replace those that are lost or damaged.

InTechnology will supply a small number of Hardware tokens at the start of the contract that can be used as advance replacement for faulty tokens. When this stock has depleted, the customer must return the faulty

tokens, and InTechnology will replenish the stock. (one spare provided for every 25 hardware token licenses ordered)

Customers with a large estate of hardware tokens are advised to order ‘spares’ as part of the initial order for use as replacements for lost or damaged tokens.

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

Off-boarding processes/scope

N/A

Out of Scope features

None.

SERVICE MANAGEMENT

InTechnology Plc utilises InTechnology Managed Services (Redcentric) to provide its service support. The support provided by Redcentric is detailed below.

Service Support

Redcentric will monitor and manage of the service elements hosted centrally to support the service.

Redcentric's customer service operation is available 24/7/365 and can be contacted by telephone, email or via the customer portal. The customer call is routed directly to the Service Management Centre (SMC) who will log your service call, agree the call priority and assign a customer interaction number which will allow your request to be identified efficiently and tracked at all times.

Redcentric has one direct point of contact for customer support, which deals with all aspects of the Service. The Redcentric Customer Services team takes full responsibility for supporting and logging problems and technical support queries. Their specific role is to ensure that all telephone, email and portal queries are answered and resolved as promptly as possible.

They will provide the customer with a customer interaction number and the engineer will then deal directly with the query. The customer interaction number is useful to quote if making enquiries to the progress of the call and it also helps Redcentric monitor the progress of that call. Redcentric employs over 470 staff, 80% are customer facing.

The skills vary from server and storage specialists (EMC, NetApp and Isilon), to Microsoft and VMware specialist, to network and routing specialists (Cisco, Riverbed etc), data management and protection specialists (e.g. Symantec, IBM, i365, etc).

All services 24/7 managed and monitored

The proposed solution costs are inclusive of Redcentric's support and account management processes and include:

- Genuine 24 / 7 / 365 support, manned, monitored and maintained.
- UK based technical support.
- Best in class secure monitoring tools, designed to ITIL guidelines.
- Customer reference site for HP .

Service Management

Redcentric prides itself on the service that it provides to its customers; an assigned account management team will be provided from the outset, the account team consists of a Client Account Manager (CAM), and a Service Manager (SM).

Specifically, Redcentric's Customer Account Managers will:

- Be the client advocate – Redcentric's Account Management team is measured and rewarded against client satisfaction
- Provide an empowered point within Redcentric to which issues surrounding satisfaction of service may be escalated and resolved
- Offer assurances that Redcentric will be acting in their interest at all times

- Act as a single point of contact for all non-technical issues - working collaboratively at all times with the Client Account Manager to develop a thorough understanding of your business needs and growth. Through understanding the Client's goals and the technology that is used, we are able to give proactive recommendations that are customer / site specific and will facilitate and support growth

- Act as a communication channel – the Service Manager (SM) will be the key point of contact for Clients wishing to develop their critical applications or infrastructure. They are responsible for organising meetings and / or conference calls with developers, systems integrators and Redcentric staff to discuss performance and upgrades.

- Troubleshoot and provide problem resolution – although the Client Support Desk will provide immediate technical assistance for faults, the Technical Relationship Manager will co-ordinate medium-term projects with the intention of resolving recurring problems should they arise.

- Provide trusted advice – the Redcentric Account Management Team becomes an extension and trusted advisor of the Client's IS/IT department and will foster additional business relationships with the client to achieve common goals.

- Take a proactive approach – the Redcentric Account Management Team will take a proactive approach to the Client's critical application or infrastructure environments.

SERVICE CONSTRAINTS

Maintenance Windows

Redcentric is committed to continually improving and expanding its core network and data centre capabilities, thus striving to provide the highest levels of service to its customers. In order to facilitate these improvements, it is necessary to carry out essential work from time to time. These activities are carefully scheduled through the use of an internal change control process which is designed to present maximum visibility of that change and thereby ensure that planning and implementation are carried out to minimize the effect on customers and their network services.

For the benefit of our customers Redcentric will allocate a pre-determined planned window which will be utilised to carry out any core infrastructure changes which may carry a minimal risk of disruption to service, or in some instances a period of service downtime which would be kept to an absolute minimum. In either instance, customers will be notified of the full details of the requirement with a minimum of 14 days' notice prior to the maintenance window. Generally Redcentric will endeavour to carry out any improvements in the reserved windows listed below; however unforeseen circumstances might dictate that improvements are carried out at other times. Notwithstanding such notice Redcentric shall still provide the Services in accordance with the applicable Service Level.

Redcentric will endeavour to give customers as much notice as possible.

In very exceptional circumstances, there may be an emergency requirement to instigate work outside of these maintenance windows, however, every effort will be made to avoid disruption during core service hours and prior notification will be issued at the earliest possible opportunity.

There may be occasions when there is a requirement for an Emergency Change to be carried out (e.g. a hardware failure to a core network device which has caused loss of resilience). Emergency Change allows for Change to be fast tracked with <14 days customer notification. Emergency Change is only used in exceptional circumstances, where there will be a significant business impact should the change not be expedited. Emergency Change records are thoroughly reviewed by the Redcentric Change Advisory Board (CAB) to assure they were justified.

Level of Customisation Permitted

InTechnology Managed Services will configure the service based upon requirements set by the customer; elements of the service which can be customised include;

- IP addressing
- Access Control Lists (ACL)
- Encryption options

Schedule For Deprecation Of Functionality/Features

Service Restrictions

- No access to the HSCIC Healthcare Network from outside England is permitted over the InTechnology aggregated service.
- InTechnology will only provide access to the HSCIC Healthcare network for an organisation with whom it has a direct contractual relationship; access to the network cannot be sub-contracted or "re-sold".
- No Person Identifiable Data may be viewed, stored or processed by any connected party outside of the boundaries of England without the express written permission of the NHS.

Service Levels

InTechnology understand the importance of the services that our Customers are looking to contract for as defined within your requirements.

InTechnology already have SLA's and Penalties (service credits) as standard offerings for each of our managed services.

Availability

The Service Level applicable to the N3-SRA Service is as follows:

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

Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in Terms and Conditions 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 N3 connectivity or services.

Floor Service Level

The Floor Service Level applicable to the N3-SRA Service in respect of Availability shall be 85% in any given Month.

Service Credits

The Service Credits applicable to the N3-SRA 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 N3-SRA 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

Support Hours

The Customer Service operation is available 24x7x365 and can be contacted by telephone, email or via the Customer Portal. Your call is routed directly to our Service Management Centre (SMC) who will log your Service Call, agree the call priority and assign a customer interaction number which will allow your request to be identified efficiently and tracked at all times.

Severity Definitions

The following table defines examples of the priorities to be used by the Customer and Redcentric when logging calls. Redcentric shall respond to all requests for support in accordance with the table on the following page:

Priority 4 (Low)	Typical Event
Classification: • Monitoring of an open Incident.	• Monitoring Phase if required for a previously categorized P1-P3 Incident (for example health-check/performance monitoring of a customer's CPE). • Not to be treated as Advice and Guidance as this should be an Interaction. Redcentric call handling process: Logged service calls will be progressed between the hours of 09:00 - 17:30 hrs until
Priority 3 (Medium)	**Typical Event**
Classification: Single user issue but not a VIP. • Call Logging: 24hr x 7 day x 365 days • Response: Within 1 business day	• Admin change of one users Broadsoft account. Redcentric call handling process: Logged service calls will be progressed between the hours of 09:00 - 17:30 hrs until resolved.
Priority 2 (High)	**Typical Event**
Classification: Error or fault with the installed product or service but which has no critical effect. Operational but degraded product or service. Temporary work-around may be available • Call Logging: 24hr x 7 day x 365 days • Response: Within 4 Hours - 24x7x365	• Backup task/agent failure • Remote LAN/WAN circuit errors or IP packet loss • System performance degraded • Non specific fault or problem Redcentric call handling process: Logged service calls will be progressed 24x7x365 until resolved

Priority 1 (Critical)	Typical Event
Classification: Error or fault with the installed product or service, which is causing severe impact to Customer operations. Product or Service unusable. Major incidents. • Call Logging: 24hr x 7 day x 365 days • Response: Within 1 hour - 24x7x365	• Escalation of Priority 2 call • Complete failure/unavailability of backup service • Data Circuit failure • Customer unable to connect to Internet • Major problem with firewall • System Failure Redcentric call handling/escalation process: Logged service calls will be progressed • 24x7x365 until resolved Routine notification to Team Leader

"Typical events" are illustrative only and are not limited to the events listed.

Service Credits

The Parties agree that the payment of Service Credits is a reduction in Charges for the receipt of a deficient Service and that Service Credits are the only remedy for failure to meet a Service Level. The Service Credits are calculated by reference to the Charges for the Service affected.

Availability and Performance Calculations

The availability Service Level is calculated at the end of each Measurement Period and is calculated as follows:

$$Percentage\ Availability = \frac{(MP-SU)x100}{MP}$$

Where:

MP = Measurement Period. This is the total number of minutes in the measurement period.

SU = Service Unavailability. This is the total number of minutes in the measurement period when the Service is not available for use by the Customer for reasons other than those set out below.

The following events shall be excluded from any assessment of Service unavailability:

Service unavailability due to the acts or omissions of the Customer or its employees, agents or subcontractors (excluding Redcentric).

Service Specific details

If the availability of a site, measured over 12 months, is lower than the committed figure, a proportionate amount of the annual charge will be refunded by way of a service credit. The proportion will be the committed availability percentage minus the achieved availability percentage. For example, if the committed availability is 99.5% and the achieved availability is 99.0%, the service credit is 0.5% of the annual charge.

Training;

InTechnology will provide a User Guide and an Administrator's guide. In addition, InTechnology will provide telephone support as the customer adds the first few users to the system via the administration portal if necessary.

Ordering and invoicing process

Services are billed monthly in arrears.

Payment can be via:

- Purchase Order
- BACS

Termination terms

InTechnology will provide assistance where possible to facilitate a transition to any replacement service.

InTechnology will not be obliged to disclose any confidential information to the customer or replacement supplier, or to transfer any assets, contracts, employees or third party licences.

InTechnology will provide an inventory of all data relating to the services that is under the control of the InTechnology.

InTechnology will transfer all the customer data relating to the services to the customer.

At the end of the contract with the customer and if the customer does not wish to renew their service.

InTechnology will assist the Customer in facilitating the orderly transition of the InTechnology Services (in whole or part) from InTechnology to the Customer or any replacement supplier upon the expiry or earlier termination of the agreement. This section sets out the principles regarding the service transition that form the base of an Exit Plan.

InTechnology shall produce an Exit Plan upon notification of termination of the agreement, in accordance with the principles set out in this section, as soon as practicable (but not later than 60 days) after any notice of termination of the agreement.

Exit Plan

The Exit Plan shall, unless otherwise agreed with the Customer:

- address each of the issues set out in this Exit Plan in order to assist the Customer in facilitating the transition of the InTechnology Services from InTechnology to a replacement supplier or the Customer ensuring to the extent reasonably possible that there is no disruption in the supply of Services and that there is no deterioration in the quality of delivery of the Services during any period of transitional assistance;

- provide an estimate of the scope of transitional assistance that may be required by the Customer and suggest how such assistance might be provided (if required); and

- provide an estimate of InTechnology's personnel that may be required to provide transitional assistance and suggest the management structure to be put in place and employed to provide such transitional assistance.

Agreement Termination

On termination or expiry of the Service Agreement, the Customer must undertake the following responsibilities:

- agree a time and date for the Customer's equipment to be removed; and then

- remove the Customer's equipment at the agreed time on the agreed date in a sequence to be specified by the Customer

Additional Transition Assistance

Where the Customer requests the provision of additional transitional assistance, in addition to that required under the section, InTechnology shall provide such assistance as an additional service. The additional transitional assistance detailed here shall be chargeable at the InTechnology prevailing time and materials consultancy day rates.

The transitional assistance shall, at the Customer's option, include any one or more of the following, but in each case only in relation to assets which are the subject of the InTechnology Services:

- notifying the Customer or replacement supplier of procedures to be followed and providing management to ensure these procedures are followed in relation to the transfer of the InTechnology Services;

- providing assistance and expertise as reasonably necessary to identify all material operational and business processes (including all supporting documentation) used by it or the Customer or replacement supplier in the provision of the transferring InTechnology Services;

- documenting the current status of work in progress and transferring such work in progress, including any partly completed developments and any partly completed Service Agreement changes to the Customer or any replacement supplier;

- to the extent that InTechnology is reasonably able to do so, providing assistance and expertise as reasonably necessary for examining all relevant roles and responsibilities in place for the provision of the InTechnology Services and the transitional assistance;

- providing information within InTechnology's possession about capacity and performance requirements;

- providing reasonable assistance to the Customer in procuring and receiving replacement services;

- co-operating in the execution of the plan for the migration of the Customer data (if any) compiled or used in the performance of the Services to the Customer or the replacement supplier providing skills and expertise of a suitable standard;

- assisting the Customer and the replacement supplier in the execution of a parallel operation involving the provision of the InTechnology Services (in whole or part) at the same time as the replacement services;

- the provision of all reasonable assistance required by the Customer to ensure the smooth transfer of the InTechnology Services to the Customer or the replacement supplier;

- providing any technical advice as may be reasonably required by the replacement supplier or the Customer to facilitate the provision of the replacement services to commensurate service levels and standards to those required by this Service Agreement; and

- answering all reasonable questions including requests for technical advice from the Customer or its replacement supplier regarding the general nature of the Services.

Responsibilities;

Customer Responsibilities

The customer is required to successfully complete the Information Governance process prior to being permitted to gain access to either the N3 or any N3 resources. In addition;

- Distribution , set-up and support of remote VPN software to individual users
- Identifying and sourcing suitable IP-sec compliant client software for device / operating systems combinations not supported on the supplied software
- Adding user details to the platform, and allocating each user a token license
- Trigger the software token allocation for each user or physically allocate hardware tokens to users
- Undertake user support and administration using the Administration Portal (eg. user password re-set)
- Return faulty hardware tokens to InTechnology (in batches)
- Make provision for suitable Internet connectivity for end users

InTechnology Responsibilities

InTechnology is responsible for the following activities;

Configures the customer environment on the remote access and authentication platforms

- Loads token licenses onto the platform
- Provides the customer with sample VPN client software
- Dispatches hardware authentication tokens to a single customer location usually in a single shipment
- Configures the platform to access N3 resources as per the pre-sale design
- Maintains the resilient centralised authentication and remote access platforms

Technical requirements

Service dependencies

The customer is required to provide the following information to provision N3 Gateway Services

- IP addressing
- ACL configuration
- Encryption characteristic (if applicable)

Detailed technical interfaces,

e.g. client side requirements, bandwidth/latency requirements etc.

There are no detailed technical interface restrictions to provision the service other than sufficient client side switch / router port capacity be required to terminate the service connections.

Details of any trial service available.

No trail service can be provided.