Unity On a SIM

Service Definition

SD074 v1.5
23/08/2020

redcentric

AGILE • AVAILABLE • ASSURED

1 SERVICE OVERVIEW

The Unity on a SIM service enables customers to take an unlocked mobile handset, or SIM enabled desk phone and turn it into a fully functioning business phone, with DDI numbers, short-dial extensions, call transfer, hunt groups, IVR, voicemail, shared call appearance and all the other Unity features you would expect.

This service works natively from a SIM and is not an OTT (Over the Top) app, therefore, any unlocked handset can be readily integrated into a customer's existing Unity estate.

2 SERVICE DESCRIPTION

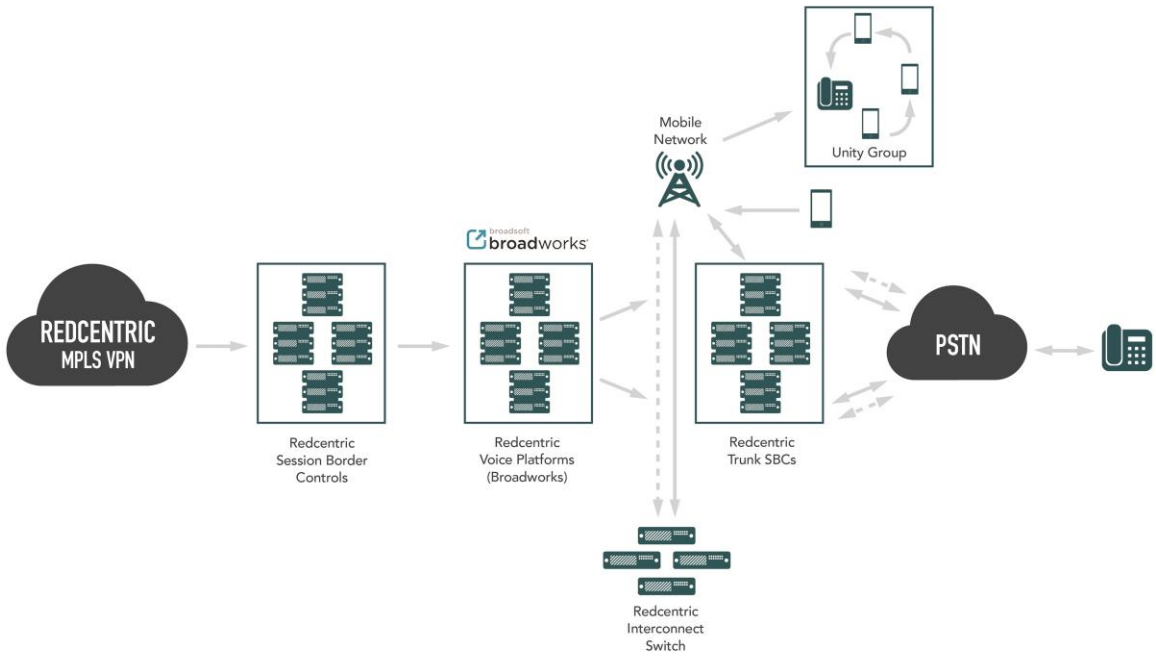


FIGURE 1 – UNITY ON SIM ARCHITECTURE

2.1 FEATURES

All features as currently provided available on the Unity platform can be utilised by the Unity on a SIM service.

- Calls and Data
- SMS on mobile numbers or text enabled Geographic numbers*
- Multi-format SIMs
- Landline and mobile numbers
- Port your own number
- Redcentric or customer branded network (excluding iPhone)
- All standard features and functions of the Unity IPT service

* *must be a new geographic number provided by Redcentric.*

2.2 BENEFITS

- Rapid deployment - No installation. Any unlocked handset capable of 2G/3G/4G
- Call Recording - Recordings can be accessed via our easy-to-use web portal
- Never miss a call Voicemail to email, call forwards, transfers, diverts & out-of-hours routing
- Productivity everywhere Single number reach, UK and worldwide
- Secure and compliant No insecure network as it doesn't run via an app. Network call recording & inclusive disaster recovery
- Advanced integration Call centre, call dashboards, video & unified communications Licensing
- Roaming Both UK & international (profile dependent)
- Simplified Single voice profile for fixed line and mobiles

2.3 LICENSING

The Unity on a SIM service is delivered utilising in conjunction with the standard core Unity service packs. Additional licences are adding via the standard contract process.

- Shared call appearance required
- Minimum requirement is the Redcentric Enterprise service pack licence

2.4 SERVICE ORDERING

The Unity on a SIM service is ordered by way of Redcentric's standard contract process. Subsequently, orders can be placed by authorised person completing the online information via Redcentric's "Inform" portal.

It must be stated at point of order if a new text enabled number is required.

Orders can be placed using the following part code(s):

2.5 CORE SERVICES

Part Code	Description	Pricing Notes
N-UOS-301	Unity on a SIM Setup	One off charge/Per SIM
N-UOS-402	Unity on an MultiNet 4G SIM Unlimited 2GB	Monthly Rental - Roaming
N-UOS-403	Unity on an MultiNet 4G SIM Unlimited 4GB	Monthly Rental - Roaming
N-UOS-404	Unity on an MultiNet 4G SIM Unlimited 10GB	Monthly Rental - Roaming
N-UOS-405	Unity on an MultiNet 4G SIM Unlimited 20GB	Monthly Rental - Roaming
N-UOS-406	Unity on an MultiNet 4G SIM Unlimited 40GB	Monthly Rental - Roaming

Note: *out of bundle charges apply as detailed on the price sheet.*

2.6 ONBOARDING PROCESS

Redcentric's onboarding comprises of a project managed, five phase technical and business consultative process.

Phase 1 - Redcentric presales will work with the Customer to clearly capture & document the current requirement(s).

Phase 2 – The provisioning team will activate the SIM(s) via the web-based portal

Phase 3 – Service delivery will add the device to the Customer's Unity account and apply the required features

Phase 4 – The SIM, and device if applicable, will be shipped to the Customer

Phase 5 – Test calls will be made to the new user device

2.7 DECOMMISSIONING PROCESS

Upon expiration of the contract where the Customer chooses not to renew with Redcentric, the following steps are followed as part of the decommissioning process:

Phase 1 – Contractual - Expiration of the service contract, or the Customer decides not to renew. This may also include early termination by the Customer, subject to payment of early termination fees.

Phase 2 – Port out requests will be actioned

Phase 2 – Service Decommissioning

Phase 3 - Removal of user accounts/devices from the platform.

Note: SIMs will remain the property of Redcentric and must be returned as part of service decommissioning process.

2.8 TECHNICAL REQUIREMENTS

- The service is compatible with any unlocked UK compatible 2G/3G/4G GSM handsets

2.9 RESPONSIBILITIES

2.9.1 CUSTOMER

- Provide an unlocked GSM handset or device capable of 2G/3G/4G if not supplied by Redcentric

2.9.2 REDCENTRIC

- Add the device to the Customer's Unity account
- Apply features/service pack
- Ship the SIM to the address requested
- Supply and ship the handset/device if included on Customer contract

2.10 CUSTOMER DEPENDENCIES

It's the Customer's responsibility to:

- Provide or purchase a suitable device
- Accurately report any service-related faults

2.11 SECURITY BEST PRACTICES

The purpose of this section is to detail the potential security risks associated with the operation of any phone system and to provide information and requirements on how to minimise these risks when using the Call2Teams service.

Security and privacy must focus on controlling unauthorised access or excessive access to features within the voice platform.

It is imperative that you ensure the correct level of security is implemented on your organisation's configuration to prevent fraudulent use of the Service. Fraudulent use can result in additional call costs to your organisation if the appropriate security measures are not implemented.

It's your organisation's responsibility to ensure adequate security practises/processes are followed and that the appropriate security measures are implemented. The security requirements in the following document are subject to constant review and improvement.

2.11.1 Background: How Phone Systems are attacked

Inherent within any voice system is the potential for abuse. The methods through which a service can be abused include the following:

- Unauthorised remote access to a telephony system in order to:
  - Make expensive calls at zero cost to themselves
  - Make calls to premium rate numbers to fraudulently generate revenue
  - Unlawfully intercept confidential information such as voicemail messages

- Deliberate and direct misuse by staff including:
  - Making expensive calls whilst at work to save on their own bill
  - Fraudulent use of call forwarding – when users misuse their call forwarding services to make long distance or premium rate calls by dialling their own number from outside the office
  - Calling premium rate numbers to generate revenue for themselves / another

- Inadvertent direct misuse by staff including:
  - Being coerced or tricked into dialling premium rate numbers
  - Being coerced or tricked into providing a service for fraudsters (such as through call forwarding)

- Deliberate remote misuse by staff including:
  - Dialling into the phone system from outside the office to make non-business or fraudulent calls
  - Accessing the system using a voice service web portal or software application to make non-business or fraudulent calls

Hackers are constantly looking for ways to access telephony systems via a user's account with a view to scanning the options for a means of making outbound calls. The Customer ends up bearing the costs of these calls, which are often made to expensive premium rate or international numbers. Details of how to hack into telephone systems are even posted on the Internet.

Ensuring that each user's password is hard to deduce is the primary method to combating the fraudsters.

If a hacker accesses a system, fraudulent abuse may take the form of:

- Accessing a user's account and establishing an onward call from the system.
- Accessing a user's account, setting the call forwarding to an external number (such as a premium rate dialling service) and then calling the user's number at a local rate.
- Interception of the user's confidential voicemails.

All these attacks are preventable with the adoption of a simple voice security policy. It is imperative that adequate security is implemented on your organisation's telephony configuration to prevent this.

It is important to note that the following configuration elements including the definable policies are included within your security policy.

1. Group Administrator and end-user Passwords
2. End-user voice-mail passcodes
3. Outgoing Calling Plan
4. Making outgoing calls through the voice-mail portal
5. Housekeeping (managing new and redundant user accounts)

2.11.2 Group Administrator and End-User Passwords

The Group Administrator (responsible for management of the Unity IP Voice Service at Group level) and users require passwords to access the web admin portal. This portal provides the group admin with administrator privileges, allowing them access to manage the Unity IP Voice Service and configure users and features. This portal also provides users with access to configure and manage their own individual features. The user passwords are also used by users to log in to the voice service software applications.

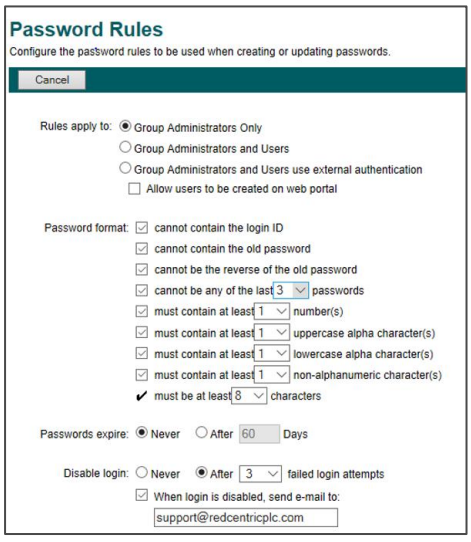
Unauthorised access to the portal at either group or user level would have significant security consequences and as such Redcentric require the following:

- Passwords must be at least 8 characters in length
- Passwords must contain at least:
  - One number
  - One uppercase character
  - One lowercase character
  - One non-alpha numeric character
- Password ageing is enabled by default at system level. *
- The limit for password retries lock-out is set to 3 or less to prevent multiple systematic retries.
- The e-mail address to which account lock-out notifications are sent is constantly monitored.

NOTE: Customers who do not wish to enable password ageing by default will be required to sign a customer waiver prior to Redcentric disabling this feature. The waiver can be accessed by calling the support desk.

2.11.3 Password Rules

The group administrator can manage password rules as follows:



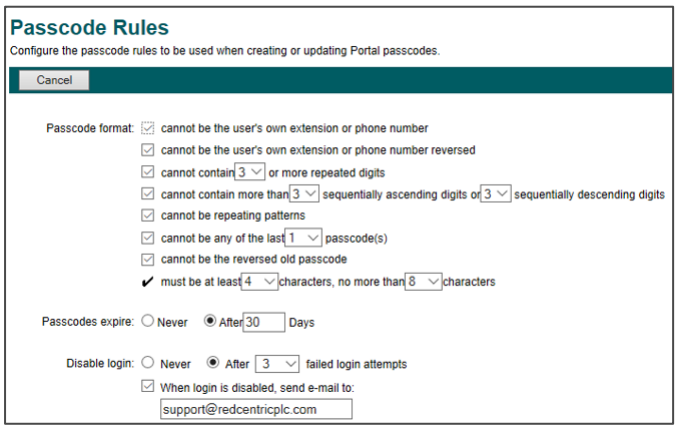
2.11.4 End-User Voice-Mail Passcodes

The easiest way for hackers to access a telephone system is by selecting a user number then trying ‘easy’ passcodes to gain access to the menus. Because of this, Redcentric require the following voicemail passcode rules are followed:

- Passcodes cannot be the user's own extension or phone number
- Passcodes must not be repeating digits such as “1111” or “2222” etc.
- Passcodes must not use “1234” or use their extension number.
- Passcodes must be a minimum of 6 digits
- The limit for passcode retry lock-out is set to 3 or less to prevent multiple systematic retries.
- Ensure the e-mail address to which account lock-out notifications are sent is constantly monitored.

2.11.5 Passcode Rules

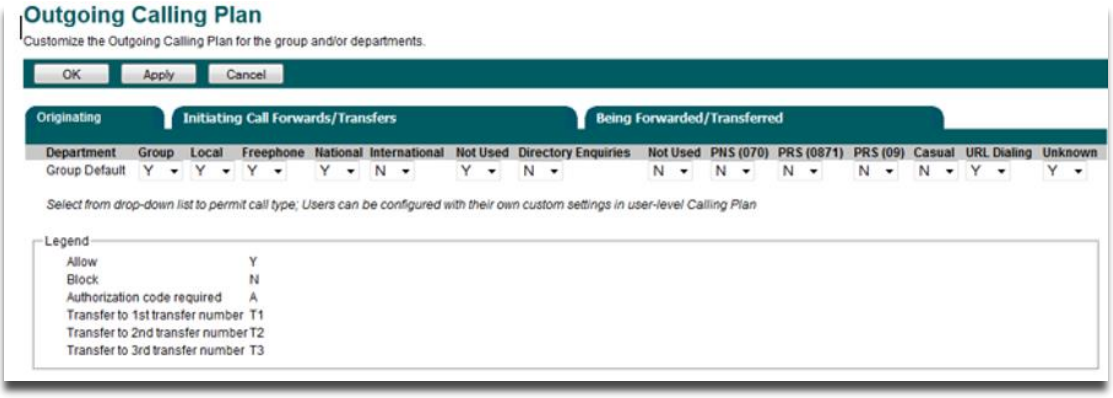
A screenshot of the passcode rules screen in which the group administrator can manage passcode rules follows:



2.11.6 Outgoing Calling Plan

The Outgoing Calling Plans (OCP) dictate what types of telephone numbers can be dialled by users. This includes originating (making) calls, and what numbers users can forward or transfer calls to. The OCPs are set and managed by the Group Administrator via the web admin portal. This feature can specify calling plans for the entire group, or individual departments. Redcentric strongly recommend that only the minimum number of call types are permitted. **Redcentric also recommends that calls to premium rate numbers and international destinations are barred.**

A screenshot of the Outgoing Call Plan screen for originating calls below:



Screenshot of the Outgoing Call Plan screen for initiating call forwards / transfers below:

NOTE: The Outgoing Calling Plan can be configured down to a specific user level. It is therefore important to ensure that Outgoing Calling Plans are carefully managed and maintained by the group administrator.

2.11.7 Default Outgoing Calling Plan

Redcentric will provision the IP Voice Service with a default Outgoing Calling Plan. This is configured as below in the interests of security. Customers requiring the ability to call destinations prohibited by the default Outgoing Calling Plan will need their group administrator to enable the required destinations.

Call Type	Policy
Group Calls (calls within the Unity Group)	PERMITTED
Local Calls	PERMITTED
National Calls	PERMITTED
Freephone Calls	PERMITTED
International Calls	NOT PERMITTED
Directory Enquiries	NOT PERMITTED
PNS 070 (Personal Number)	NOT PERMITTED
Premium Rate (0871)	NOT PERMITTED
Premium Rate (09)	NOT PERMITTED

TABLE 4: DEFAULT OUTGOING CALL PLAN

NOTE: Currently there is no option to bar mobile calls which are permitted.

2.11.8 Restricted International Destinations

In the interests of minimising the risk of fraudulent calls, Redcentric has barred access to the following high-risk international destinations.

Country Code	Destination	Country Code	Destination
0020	Egypt	00509	Haiti
00211	South Sudan	0051	Peru
00212	Morocco	0052	Mexico
00213	Algeria	0053	Cuba and Guantanamo
00216	Tunisia	0054	Argentina
00218	Libya	0055	Brazil
00220	Gambia	0056	Chile
00221	Senegal	0057	Colombia
00222	Mauritania	0058	Venezuela
00223	Mali	00590	Guadeloupe
00224	Guinea	00591	Bolivia
00225	Ivory Coast	00592	Guyana
00226	Burkina Faso	00593	Ecuador

Country Code	Destination	Country Code	Destination
00227	Niger	00594	French Guiana
00228	Togo	00595	Paraguay
00229	Benin	00596	Martinique
00231	Liberia	00597	Suriname
00232	Sierra Leone	00598	Uruguay
00233	Ghana	00599	Netherlands Antilles
00234	Nigeria	0060	Malaysia
00235	Chad	0062	Indonesia
00236	Central African Republic	0063	Philippines
00237	Cameroon	0065	Singapore
00239	Sao Tome and Principe	0066	Thailand
00240	Equatorial Guinea	00670	East-Timor
00241	Gabon	00672	Australian External Territories
00242	Congo	006721	Antarctic
00243	Republic of Congo	006723	Norfolk Island
00244	Angola	00673	Brunei Darussalm
00245	Guinea-Bissau	00674	Nauru
00246	Diego Garcia	00675	Papua New Guinea
00248	Seychelles	00676	Tonga
00249	Sudan	00677	Solomon Islands
00250	Rwanda	00678	Vanuatu
00251	Ethiopia	00679	Fiji
00252	Somalia	00680	Palau
00253	Djibouti	00681	Wallis and Futuna
00254	Kenya	00682	Cook Islands
00255	Tanzania	00683	Niue
00256	Uganda	00684	American Samoa
00257	Burundi	00685	Western Samoa
00258	Mozambique	00686	Kiribati Republic
00260	Zambia	00688	Tuvalu

Country Code	Destination	Country Code	Destination
00261	Madagascar	00689	Tahiti
00262	Reunion	00690	Tokelau
00263	Zimbabwe	00691	Micronesia
00264	Namibia	00692	Marshall Islands
00265	Malawi	0081	Japan
00266	Lesotho	0082	Korea Republic
00267	Botswana	0084	Vietnam
00268	Swaziland	00850	Korea
00269	Comoros and Mayotte	00853	Macao
0027	South Africa	00855	Cambodia
00290	St. Helena	00856	Laos
00291	Eritrea	00880	Bangladesh
00297	Aruba	00886	China-Taiwan
00298	Faroe	0092	Pakistan
00354	Iceland	0093	Afghanistan
00355	Albania	0094	Sri Lanka
00370	Lithuania	0095	Myanmar
00371	Latvia	00960	Maldives
00372	Estonia	00961	Lebanon
00375	Belarus	00962	Jordan
00377	Monaco	00963	Syrian Arab Republic
00380	Ukraine	00964	Iraq
00381	Serbia	00965	Kuwait
00382	Montenegro	00966	Saudi Arabia
00383	Kosovo	00967	Yemen
00385	Croatia	00968	Oman
00386	Slovenia	00970	Palestine
00387	Bosnia and Hercegovina	00972	Israel
00389	Macedonia	00974	Qatar
00420	Czech Republic	00975	Bhutan

Country Code	Destination	Country Code	Destination
00421	Slovakia	00976	Mongolia
00500	Falkland Islands	00977	Nepal
00501	Belize	0098	Iran
00502	Guatemala	00992	Tajikistan
00503	El Salvador	00993	Turkmenistan
00504	Honduras	00994	Azerbaijan
00505	Nicaragua	00995	Georgia
00506	Costa Rica	00996	Kyrgyz Republic
00507	Panama	00998	Uzbekistan
00508	St. Pierre		

TABLE 5: RESTRICTED INTERNATIONAL DESTINATIONS

NOTE: The restricted international destinations are barred at system level. Even with international calls permitted by the group administrator on the Outgoing Calling Plan, these destinations will still be barred.

If the Customer needs to make calls to any of these high-risk international destinations, barring can be removed by submitting a request to Redcentric support.

NOTE: that this will remove barring to all high-risk international destinations as defined above. It is not possible to permit / bar individual high-risk international destinations.

2.11.9 Making Outgoing Calls Through the Voicemail Portal

This feature allows staff to make phone calls through the same portal that they use to pick up their voicemails. This can beneficial to certain types of employee but also represents a security risk because it allows outgoing calls to be made by anyone that has been able to guess an employee's voice-mail passcode.

Because of this potential fraud risk, Redcentric do not enable this feature on any user accounts and it is Redcentric's strong recommendation that this service remains disabled. Due to the significant scope for fraudulent use, Redcentric will request a written waver of liability from the Customer before re-activating this service.

2.11.10 Authorisation Codes

The Authorisation Codes feature in Unity allows an administrator to enforce that a user enters a security code before they are permitted to make a call. This is primarily intended for public area phones but may also be used to prevent calls being made from any phone without first entering a security code.

2.11.11 Housekeeping

On new installations, new user accounts are normally created by the Redcentric service delivery team. Customers are also able to change passwords away from those initially set by Redcentric at any stage after deployment of the Voice Service. Customers may also configure new user accounts following installation after purchasing the user licences. Passwords and passcodes that are generated must always be secure (i.e. not 0000, 1234 etc.).

A redundant account with an easy to deduce password is the ideal vehicle for a hacker to fraudulently use the system and could remain undetected for a long time. The former employee could also continue to use the account (or pass on the details) at the organisation's expense. Redcentric recommends:

- Disable all visitor accounts when not required.
- Ensure that test or demo accounts are disabled when not in use or that they follow the strict password regime mentioned above.
- Remove all leaver accounts immediately or change the password.

NOTE: Redcentric will delete devices that have not connected/registered to the service for 90 days

2.11.12 Supplemental Security Recommendations

- Remove or de-activate all unnecessary system functionality.
- Review your bills regularly to spot any increases in call volumes or calls to suspicious destinations.
- Disable all surplus user accounts until you have a user for them.
- Only give individuals the appropriate and minimum level of system access they need to carry out a specific task i.e. Service Packs.
- Restrict access to your core communications equipment, such as your main computer room to avoid physical access to network switches. Hackers can intercept calls and reroute them, capture the data for later playback of the conversation or listen in on the call to capture the conversation in real time.
- Ensure that network switches are deployed within secure locations as opposed to network hubs to remove the threat of eavesdropping from within the network using PC based devices.
- Ensure that telephony devices are segmented from data devices by using the appropriate VLAN configurations
- Continually review these security recommendations at regular intervals.

2.12 REDCENTRIC SERVICE LIMITATIONS

- The service requires the Customer to have a **Minimum** 4-digit dialling plan.
- Native GSM 3 -way calling is currently not supported.
- Call Transfer is currently not supported
- Video Calling is currently not supported.
- Flexible Seating is currently not supported.
- Music on Hold is currently not supported
- Call Waiting is currently not supported.
- 2 Stage Dialling is not supported

2.13 IDENTIFIED SERVICE BEHAVIOURS

SB1: It has been identified that a User's CLI Presentation may vary depending on the calling scenario. Table 6 provides a list of the identified scenario's and expected CLI behaviours.

Call Scenario	CLI Presentation
Unity Mobile User to PSTN	Broadworks Call Processing Policies will dictate what CLI is presented based on configuration
Mobile User to a Broadworks Unity 3rd Party SIP Device – Extension Call	Broadworks Call Processing Policies will dictate what CLI is presented based on configuration
Unity Mobile User to Unity Mobile User – no business number provisioned in Mobile Control Panel **	The Users Mobile Number is presented
Unity Mobile User to Unity Mobile User – with business number provisioned in Tango Control Web Page	Provisioned Business Number is presented
Unity User to Unity Mobile	Broadworks Call Processing Policies will dictate what CLI is presented based on configuration

TABLE 6: CLI CALLING SCENARIO'S AND CLI PRESENTATION BEHAVIOURS

**** Note Customers will not have access to the Mobile Control panel. Therefore, Redcentric are responsible for making any Mobile Control panel changes.**

3 IMPLEMENTATION & ACEPTANCE

3.1 ACCEPTANCE CRITERIA

The following Acceptance Criteria will be demonstrated during the service delivery process:

- Email notification to confirm the Service has been set up
- SIM(s), and device if applicable, shipped to Customer
- Basic test calls made to and received from the new user devices.
- Text messages sent to and made from the new SIM
- Mobile data sessions established from the new SIM

4 SERVICE LEVELA & SERVICE CREDITS

4.1 SERVICE LEVELS

There are no Service Levels applicable to the Unity on a SIM service, because performance and availability depend upon numerous factors including the performance of the mobile networks, the number of users per site and mast location.

4.2 SERVICE CREDITS

No Service Credits are applicable to the Unity on a SIM service.

5 DATA PROCESSING

5.1 DATA PROCESSING SCOPE

- Redcentric does not access, alter or use any application data that is running on the Unity on a SIM Service except as specifically stated below.
- In terms of operating the Unity on a SIM service, API commands are passed into the Unity on a SIM associated supporting servers to orchestrate the build/management of identified users that have subscribed to the service.
- Users that have the appropriate role/privileges assigned to them access the Service via a secure web portal to review service settings. Note: Only users with the appropriate privileges can make changes to users under their control.
- The agreed roles and responsibilities are provisioned based on documented Customer requirements.

5.2 DATA STORAGE & UNENCYPTED DATA

- All access to data within the Unity on a SIM service is restricted via the Unity portal or via API.
- Any access to either the portal or API are controlled by HTTPS protocol, or tokenised access control.

5.3 DATA PROCESINIG DECISIONS

- In the normal course of business Redcentric does not make any data processing decisions in relation to the Service. Processing is automated and instigated by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the 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 SERVICE CONFIGURATION WITH RESPECT TO DATA

- The service configuration will be done by Redcentric as requested by the Customer.
- The initial service configuration is built using a combination of Customer provided information.
- As data controller, Redcentric hold the following information on Users on Redcentric's BroadWorks voice service delivery platform:
    - Company Information: BroadWorks Company Name, BroadWorks GroupID, Optional: Company Address
    - User Data: First Name, Last Name, Email Address, SIM Number, SIM Reference ID, Optional: Phone Number,
    - Call Metadata: Party A, Party B, Call Length, and other SIP attributes or the CDR: Time and Date, Username,
- SIMETRIC (see 5.6) below) hold the following Information on Users:
    - Company Information: BroadWorks GroupID
    - User Data: SIM Reference, SIM Number, Package Type.
    - Call Metadata: Party A, Party B, Call Length, and other SIP attributes or the CDR: Time and Date, SIM Reference ID

5.5 DATA BACKUP

- Redcentric's Core BroadWorks Voice platform backups are performed daily. Backups are encrypted during transit and stored within Redcentric's private network environment.
    - SIMETRICs platform backups are performed daily and stored on a separate, dedicated backup infrastructure
- Customers have no direct access to system backups.

5.6 SUB-PROCESSORS

- The following party is involved in delivering the Unity on a SIM service:
    - SIMETRIC: An Internet-based VPN is utilised to transit the media files between the SIMETRIC and Redcentric network.
- No other parties are involved in delivering the Unity on a SIM Service, and there are no other sub-processors appointed by Redcentric.

5.7 CUSTOMER ACCESS TO DATA

- The Customer has login rights to the Unity on a SIM service via secure web portal.
- Access to configuration is based on roles and responsibilities defined by the Customer as part of the service setup.

5.8 SECURITY ARRANGEMENTS & OPTIONS

- The core Infrastructure delivering the Unity on a SIM Service is hosted at both Redcentric and third-party locations. All locations meet physical security standard ISO27002 section 11.1 or equivalent. The Customer is responsible for ensuring the physical security at customer sites/locations, where the Service terminates, meets its needs.
- Customers have access via a secure portal to manage their own User configuration, but they are unable to interact directly with the back-end systems to modify any service wide configurations.
- Customer access to the portal uses role-based access controls (RBAC), integrated with Redcentric core voice platform

5.9 SERVICE OPTIONS

- Customers have the option to take Redcentric's Unity on a SIM Service, in which case:
    - as part of that Service, Redcentric will manage the initial Customer setup based on defined and agreed Customer requirements; and
    - the Data Processing section (Section 5) of the Redcentric Unity on a SIM Service Definition applies.

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