POL00395680

Document Title:	REMOTE SUPPORT SECURE ACCESS SERVER HIGH LEVEL DESIGN
Document Type:	High Level Design (HLD)
Document Reference:	DES/SYM/HLD/0017
Release:	Not Applicable
Abstract:	This document describes the High Level Design for the Remote Support Secure Access Server.
Document Status:	APPROVED
Author & Dept:	Elma Neil ; Shahid Latif
Internal Distribution:	
External Distribution:	

Approval Authorities:

Name	Role	Signature	Date
Ian Bowen	Architect – Team Lead		
David Sackman	Solution Design		
Allen Graham	Development		

Note: See Post Office Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

©Copyright Fujitsu Services Ltd 2007

POL00395680

0 Document Control

0.1 Table of Contents

POL00395680

©Copyright Fujitsu Services Ltd 2007

POL00395680

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	04/04/2007	Draft	
0.2	18/04/2007	Reviewed	
0.3	04/05/2007	Draft updated with review comments	
0.4	25/05/2007	Draft updated with review comments	
1.0	06/08/2007	Document for Approval at V1.0	
1.1	10/12/2007	Document changed	

0.3 Review Details

Note: Reviewer list is changed purposely for this document.

Review Comments by :	18/1/2008	
Review Comments to :	shahid.latif GRO & RMGADocument Management GRO	
Mandatory Review		
Role	**Name**	
Architecture	Ian Bowen	
Security Architect	Jim Sweeting	
System Test	Harjinder Hothi	
Optional Review		
Role	**Name**	
Programme Manager	Phil Day	
Applications Architecture		Dave Johns
Test Design	Peter Robinson	
Development	Graham Allen	
Business Continuity	Tony Wicks	
Migration Architect	Jeremy Worrell	
Test Design	George Zolkiewka	
Head of Service Management	Steve Denham	
Head of Service Change & Transition	Graham Welsh	
HNG-X Service Transition	Steve Godson	
Service Support	Peter Thompson	
Service Network	Alex Kemp	
Data Centre Migration	Martin Brett	
Infrastructure Design / Solution Design/Development	Gavin Scruby (Infrastructure & Estate Mgmt)	
Integration	David Hinde	
Testing	Peter Dreweatt	
SV&I Manager	Sheila Bamber	
Tester	Hamish Munro	

POL00395680

RV Manager	James Brett (POL)
VI & TE Manager	Peter Rickson
HNG-X Acceptance & Risk	Wayne Roberts (POL)
Integrity Testing	Alan Child
Core Services	Pat Lywood
Core Services	Ed Ashford
Core Services	Andrew Gibson
Optional Review	
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**
Project Manager	Mike Jacks
Technical Author	Trish Morris

POL00395680

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13/06/06	Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
ARC/SYM/ARC/0004	1.0	09/03/07	Remote Support and Diagnostics Topic Architecture	Dimensions
DES/PPS/HLD0001	0.1	30/11/06	Windows Server 2003 High Level Design for HNG-X	Dimensions
DES/PPS/HLD/0003			HNG-X Active Directory High Level Design	Dimensions
ARC/PPS/ARC/0001	1.0	15/02/07	HNG-X Platforms and Storage Architecture	Dimensions
DES/SEC/HLD/0001	0.1	29/03/07	HNG-X Strong Authentication High Level Design	Dimensions
DES/SEC/HLD/0003	0.1	20/03/2007	HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN	Dimensions
DES/PPS/PPD/0005	0.5	12/04/07	Platform Physical Design For Secure	Dimensions

©Copyright Fujitsu Services Ltd 2007

POL00395680

			Access Server - INF2	
SY/SOD/009	1.1	09/10/02	Secure Support System Outline Design	PVCS
TST/SYT/HTP/0005			HNG-X System Test (Infrastructure) High Level Test Plan	Dimensions
DES/SYM/HLD/0019			Third Party Support Access High Level Design	Dimensions

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.5 Abbreviations

Abbreviation	Definition
AD	Active Directory
API	Application Programming Interface
COTS	Commercial Off the Shelf
DMZ	Demilitarized zone
DNS	Domain Name System
DR	Disaster Recovery
MMC	Microsoft Management Console – framework for administration tools in Windows 2003
NIC	Network Interface Card
OOH	Out of Hours
RDP	Remote Desktop Protocol
SAS	Secure Access Server
SFTP	Secure File Transfer Protocol
SMG	Systems Management Group
SSC	System Support Centre. 3rd Line support
SSH	Secure Shell
TS CAL	Terminal Server Client Access Licence

0.6 Glossary

Term	Definition
OpenSSH	Open Secure Shell – A software suite providing encrypted communication session over a network using the ssh protocol.
Cygwin	Free software tools developed by Cygnus Solutions to allow Microsoft Windows OS to act like a Unix system.
OpenBSD	Free Unix-like operating system developed by the OpenBSD project
sudosh	A filter that can be used as a login shell to provide logging.

©Copyright Fujitsu Services Ltd 2007

POL00395680

0.7 Changes Expected

Changes
1. A prototype requirements traceability matrix is included in this HLD. This may be changed in later versions. 2. After the completion of the High Level Design work on the introduction of Sudosh the Command Logger may be taken out of this design (sections 4.4, 10). 3. Addition of missing document references (various sections, highlighted in yellow). 4. Lockdown of available windows tools based on user role (section 4.3.10) 5. Once ssh detailed design is finalised update WinSCP section (4.3.3) to confirm how it should be configured to use SFTP/SSH for connection to server... 6. How Cygwin is deployed may change.

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Copyright

© Copyright Fujitsu Services Limited (xxxx). All rights reserved. No part of this document may be reproduced, stored or transmitted in any form without the prior written permission of Fujitsu Services.

POL00395680

1 Introduction

1.1 Scope

This High Level Design sets out the design for the Secure Access Servers described in the Remote Support and Diagnostics architecture (ARC/SYS/ARC/0004). This will provide remote support access to IRE11 and IRE19 for the following user communities:

- SSC
- SMG
- ISD (Unix, NT and Network support)
- Test

The design will cover the connection method from the workstations to the SAS, the applications and clients installed on the SAS and the secure method used to connect to supported platforms.

The support workstations and laptops used to connect to the SAS are out of scope for this design and are described in (Ref. TBC)

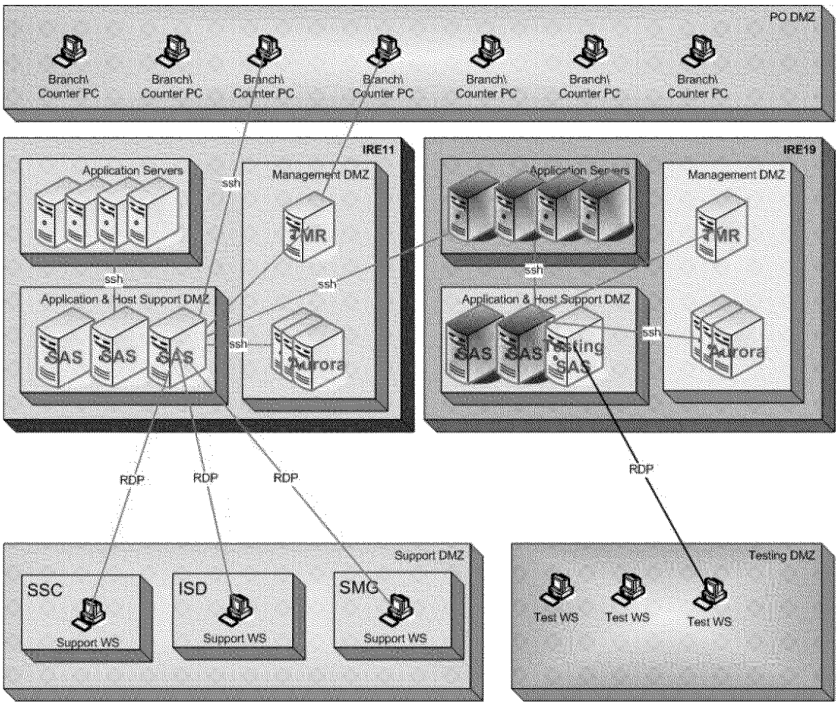
Third Party support access is not covered in this HLD. See DES/SYM/HLD/0019 - Third Party Support Access High Level Design.

1.2 Context within the Architecture

This design is contained within the Remote Support and Diagnostics Architecture. The context of the SAS is described in ARC/SYS/ARC/0004. The diagram below shows where the SAS and test SAS fit into the over all support architecture. The SAS described in this design will only be used to support HNG-X platforms. The existing Horizon SAS design will be retained to support Horizon platforms.

©Copyright Fujitsu Services Ltd 2007

POL00395680



POL00395680

2 Design Principles

Listed below are the guiding design principles for Remote Systems and Diagnostics SAS design.

- The use of COTS applications where possible with minimal bespoke development
- Role based authentication through the Identity Management System incorporating 2 factor authentication
- The SAS will provide the only supported mechanism (except for agreed emergency situations) for support staff to access the application server and counter infrastructure.
- The design needs to take account of the contractual Audit, Security and Risk procedures.

©Copyright Fujitsu Services Ltd 2007

POL00395680

3 Requirements

The high level requirements for the Secure Access Servers are to provide support teams with:

- Controlled and audited access to the operational platforms
- Multiple sessions for support users
- OpenSSH access from the SAS to the managed operational platforms.
- Secure web based access to campus servers
- Access to the System Management.

These requirements are from the Remote Support and Diagnostics topic architecture - ARC/SYS/ARC0004.

The aim of the Remote Support Secure Access Server HLD is to meet the requirements listed in **Table 1 - SAS System Requirements**, in the Requirements Traceability Section of this document.

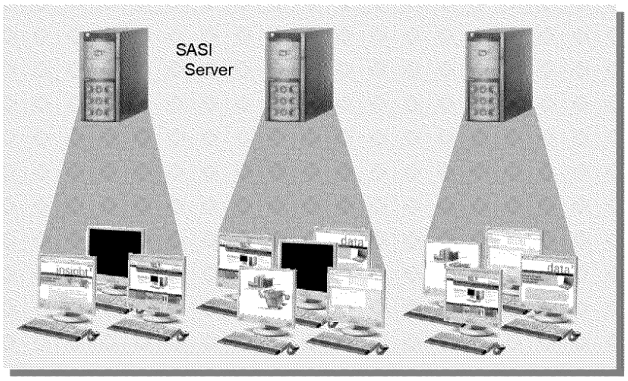
©Copyright Fujitsu Services Ltd 2007

POL00395680

4 Sub-System Description

4.1 Secure Access Server (SAS) Overview

The SAS is based on the Microsoft Windows 2003 platform as described in DES/PPS/HLD0001 - Windows Server 2003 High Level Design for HNG-X. They will be used in scale out configuration as shown in diagram below.



In this design the users are grouped and assigned to dedicated server. However, no exchange of information and no load sharing take place between the SAS servers.

4.1.1 Access

Terminal Server and Terminal Server Licensing are enabled and users will connect to the SAS using the RDP client. This will provide the ability to have more than one session to the SAS. Users will be authenticated using Active Directory and the strong authentication method described in DES/PPS/HLD/0003 - HNG-X Active Directory High Level Design and DES/SEC/HLD/0001 - HNG-X Strong Authentication High Level Design, respectively. Appropriate support roles will be configured using AD groups and policies.

System Requirement - T-RSD-3 (role based access)

System Requirement - T-RSD-9 (2 factor authentication should be used)

The Secure Shell (ssh) client will be installed on the SAS and ssh server will be installed on the operational platforms. This will provide a secure shell for support access.

OOH Support access will be provided using OOH laptops which will provide access during disaster recovery periods. The OOH laptop design is described in (add reference.)

System Requirement - T-RSD-10 (OOH access)

System Requirement - T-RSD-13 (DR support)

POL00395680

Support workstations will access the SAS using RDP and will also have the ability to access BSDB (SSC database) and the SSC server (RDP) directly. The SSC Support workstations will also be accessible from the OOH laptop using RDP. System Requirement - T-RSD-15, T-RSD-22. This is detailed in the OOH laptop design – document ref TBC.

4.1.2 Audit

All access through the Secure Access Server should be audited. A command logging service will be provided to create audit logs of all support sessions. These will be in a predefined format and collected by the Audit system and from a known file and in an agreed format.

System Requirement - T-RSD-1 (Fully logged and auditable Open Secure Shell or Open SSH facilities).

All components of the SAS should comply with the manageability requirements.

System Requirement - T-RSD-29, T-RSD-30, T-RSD-34 (Applications should provide diagnostic or log files – see manageability compliance guidelines - document ref TBC.)

4.1.3 Support and diagnostic tools

From the SAS support users will be able to run the following support tools:

- Tivoli tasks
- Cygwin tools
- Installed software clients
- Web based clients
- Windows 2003 support tools

4.2 Terminal Server

Terminal server is licensed as part of Windows 2003. License Manager is provided as part of the installation of Terminal Server. Each client accessing through the Terminal Server requires a licence (Terminal Service Client Access Licence – TS CAL) and the License Manager limits access to only licensed users or devices. “Per Device” licensing will be used.

4.3 Administration Tools

4.3.1 Cygwin

Cygwin is free software that provides a Unix-like environment and software tool set to users of any modern version of MS-Windows for x86 CPUs (95/98/NT/2000/ME/XP). Cygwin consists of a Unix system call emulation library, `cygwin1.dll`, together with a vast set of GNU and other free software applications organized into a large number of optional packages. Among these packages are high-quality compilers and other software development tools, a complete X11 development toolkit, GNU emacs, TeX and LaTeX, OpenSSH (client and server). For HNG-X we will be installing minimum set of packages to use OpenSSH client and server. Cygwin is used for connecting to servers at both datacenters and to counter machines.

©Copyright Fujitsu Services Ltd 2007

POL00395680

Cygwin has three different authentication methods, for HNG-X it is planned to have public/private for authentication.

4.3.2 OpenSSH Client

Open Secure Shell (OpenSSH) is a free implementation of the SSH connectivity tools, developed by the OpenBSD project.

OpenSSH encrypts all traffic (including passwords) to eliminate security vulnerabilities and provides secure tunnelling capabilities.

To establish an SSH session an SSH client is required on the SAS and the SSH server service or daemon on the target system. The Quest OpenSSH client (Quest-PuTTY-0.60_q1.129) will be used to connect from the SAS to the ssh server.

This is detailed in the HLD for OpenSSH/sudosh connectivity. Document ref TBC.

System Requirement - T-RSD-1

4.3.3 BSEC

For establishing the true identity of the admin/support users authorised to access HNG-X platforms, at any SAS Servers for the HNG-X project, BSEC software is installed on all SAS servers. For details refer to DES/SEC/HLD/0001.

4.3.4 Branch Router Access

All Branch Routers are accessible from Headend device in the data center and there is network connection between SAS server and Headend device. Therefore Telnet/FTP connections to Brach Router are made from SAS server. As all communication is taking place through Headend device therefore a common support userid and password will be used.

4.3.5 Secure File Transfer

No file transferring facility is provided at SAS server.

4.3.6 Web Clients

Microsoft Internet Explorer 6 sp2 will provide connection for web based clients. This access will not be audited on the SAS and access should be restricted, secure and auditable on the target server. Web clients should use https and certificates will be provides by the Certificate Authority described in DES/SEC/HLD/0003 - HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN.

System Requirement - T-RSD-2

4.3.7 EMC Client and Tools

POL00395680

EMC Centera Management Tools V3.1 is required to provide administration access to EMC infrastructure.

System Requirement - T-RSD-2

4.3.8 Microsoft SQL Server 2005 Management Studio SP2

This provides management access to SQL Server databases. This will be installed after INF2.

System Requirement - T-RSD-2

Microsoft Virtual Server 2005 R2 SP1

4.3.9 Microsoft Virtual Server 2005 R2 SP1

4.3.10 This piece of software along with IIS6.0 is required to manage Microsoft virtual servers in both datacenters. This will require TCP port 1024 to be allowed from the SAS servers into the HNG-X AD network.

4.3.11 Oracle 10g Client

The 10g client will provide access to Oracle Databases to perform custom diagnostics and for the development of bespoke interfaces. The client will provide access to oracle databases on BSDB, SSC servers only.

System Requirement - T-RSD-2

System Requirement - T-RSD-22

4.3.12 JRE6 and JDK6

Java SE Runtime Environment and the Java Development Kit have been updated to the latest supported version from Horizon. These provide a complete environment in which to run and develop Java applications

4.3.13 Tivoli Client and tools

The SAS will be used to run the Tivoli clients and tools detailed in the sub-sections below.

4.3.13.1 Tivoli Framework Endpoint (WIN_TMF_EPBASE)

The Tivoli Endpoint is the agent that resides on all managed Endpoint nodes and allows secure dialogue with the TMR. This is the Endpoint agent to allow support users to manage and remote control target systems from the SAS.

4.3.13.2 Tivoli Management Framework Desktop (WIN_TMF_TIVDT)

This is the standard Tivoli desktop needed to interact with the Tivoli Management Servers.

4.3.13.3 Tivoli Remote Control Controller (WIN_TRC_CNTTGT)

Tivoli Remote Control is an application that utilises the framework to take control of an Endpoint, It allows remote control of the mouse, keyboard and screen. This allows support users logged onto the SAS server to run remote control onto other platforms.

POL00395680

4.3.13.4 Tivoli Omnibus Software (WIN_NCO_OMNIBASE)

This package installs the Base Event software.

4.3.13.5 Netcool Omnibus Probes (WIN_NCO_PROBEWIN)

This package installs the Windows event probe on the SAS.

4.3.13.6 SMG Reboot (WIN_SMG_REBOOT)

This package installs the SMG utility providing a generic reboot task for all server platforms.

4.3.13.7 Omnibus License Server (WIN_NCO_LICSVRBASE)

This package installs the Omnibus License server needed to allow Omnibus probes and base event software to run.

4.3.13.8 Additional Tivoli Packages

- WIN_NCO_NETINTBASE- Probe Configuration Fileset
- WIN_ITM_OSAGENTBASE - Tivoli monitoring base product for operating systems
- WIN_ITM_UNIAGENTBASE - Tivoli monitoring base for universal agent
- WIN_SMG_INSTSUPPLIB - SMG installer toolset.

4.3.13.9 Tivoli Tasks

Tivoli tasks will be available to run on Data Centre platforms and Branch infrastructure (including branch router) from the SAS.

The Tivoli tools available in Horizon are being reviewed and updated for HNG-X by SMG. It is expected to have a, reduced, core set of Tivoli tasks. Custom tasks will be developed by SSC within a secure Controlled Tool Development Framework and the Ad-hoc Toolset Lifecycle. (See ARC/SYS/ARC/0004 for overview.)

These tools will be available to run from the SAS and the user's role will determine which tasks they have access to.

Add ref. to Tool Development Framework.

System Requirement - T-RSD-2 (Logged and auditable access)

4.3.14 Support tools for Windows 2003

See Appendix A for a table of available support tools for Windows 2003.

Main areas available are:

- Built in command line tools

(see http://technet2.microsoft.com/WindowsServer/en/library/552ed70a-208d-48c4-8da8-2e27b530eac71033.mspx for a full list of Windows 2003 command line tools)

POL00395680

- Support tools included with Windows 2003
- Microsoft Windows 2003 Resource Kit tools
- MCC Snap-ins with Windows 2003

Toolsets will require review and may require lockdown after INF-2.

POL00395680

5 Platforms

See the corresponding PPD – DES/PPS/PPD/0005.

5.1 Hardware

The SAS servers will be installed on VirtualBladeFrames.There will be 3 virtual Blades at IRE11, and 3 virtual Blades at IRE19 in Active – Active mode.. These servers will be used in active - active configuration at both data centers. See table below for overview specification.

Virtual Server
2 Virtual CPUs
4 GB RAM

5.2 Software

5.2.1 OS

This platform uses the HNG-X standard Windows 2003 Server OS build as described in DES/PPS/HLD/0001 – Windows 2003 Server AS HIGH LEVEL DESIGN FOR HNG-X, V0.1. Microsoft Windows 2003 Terminal Services will be enabled. Terminal Services Licensing Service will be installed on AD server and configured for 300 “per device” TS CALs ..

5.2.2 Applications

The table below summarises the software to be installed for the HNG-X SAS.

Part Name	Source	Comments
Microsoft Internet Explorer 6.0 SP2	Microsoft	
Windows 2003 platform poa_bastian.xml security policy		Part of the platform foundation build. The security policy poa_bastian.xml is supplied in the windows distribution. Installed automatically as part of the platform foundation build.

POL00395680

Microsoft SQL Server 2005 Management Studio SP2 (Available INF3)*	Microsoft	
Support tools for W2K3	Microsoft	
Antivirus software		Sophos anti-virus - Install and test with INF-1 and INF-2 platform
Oracle 10g Client	Oracle	Oracle 10g Client (Available INF3)*
SMG Tools for SAS (SMG_SRDN0484_SAS_SERV)		Confirm new versions
SSH Client (Cygwin v 1.5.24-2)		New version cygwin - uncustomised for INF2
SSH Logging server application (Available at INF3)*		Updated for HNG-X
SSH CONFIG APPLICATION (Updated at INF3)*		Updated for HNG-X
SSH SAS Configuration (Cygwin –customised by Fujitsu Services - Available INF3)*		Updated for HNG-X
NetBackup –Java Administration Console(Veritas NetBackup)		Version NetBackup (6.5)
Clariion Disk Library Console		
Microsoft Virtual Server 2005 R2 SP1		
Microsoft IIS 6.0		
WinZip		
Microsoft Excel		
Win Word		
JRE 6	Sun Microsystems	Previously Sun JRE 1.4.2_03 Download
JDK 6	Sun Microsystems	Sun Java 2 sdk 1.4.2_06 Download
Backup Solution SW	TBD	
EMC Centera Management Tools	EMC	
WIN_TMF_EPBASE (Tivoli Management Framework Endpoint)	IBM	Tivoli Framework Endpoint
WIN_TRC_CNTTGT (Tivoli Remote Control Controller / Target)	IBM	Tivoli Remote Control Controller
WIN_NCO_LICSVRBASE	IBM	Tivoli FLEXlm Licence Manager
WIN_NCO_OMNIBASE	IBM	Tivoli Omnibus Software
WIN_NCO_PROBEWIN replaces MANEVENT Filter Server	IBM	Netcool Omnibus probes
WIN_TMF_TIVDT (Tivoli Management Framework Desktop)	IBM	
WIN_SMG_REBOOT (SMG Reboot)	IBM	
SMG Tools for SAS (SMG_SRDN0484_SAS_SERV)	IBM	
WIN_NCO_NETINTBASE	IBM	
WIN_ITM_OSAGENTBASE	IBM	Tivoli monitoring base product for operating systems
WIN_ITM_UNIAGENTBASE	IBM	Tivoli monitoring base for universal agent
WIN_SMG_INSTSUPPLIB	IBM	SMG installer toolset.

POL00395680

Scheduling solution	TBD	Replaces Tivoli Maestro for NT platforms Not known

5.3 Disk Configuration

Disk configuration is from Windows 2003 server platform HLD.

For the INF-2 SAS disks will be configured as follows.

C: (systems and apps)	12.5 GB SAN
F: (pagefile)	8 GB SAN
H: Apps	12.5 GB SAN

See the corresponding PPD – DES/PPS/PPD/0005.

5.4 Backups

No backup requirements at INF-2. This will be further defined after INF-2.

POL00395680

6 Networks

Connectivity between remote support components is shown below. Please refer to the Network HLD for HNG-X.

Source	Destination	Description	Protocol	Ports
WGN01, STE09, IRE11, BRA01 workstations.	SAS	Server Support Teams, Application Support Teams and Testing Teams access SAS and Test SAS.	RDP	3389
WGN01, STE09, IRE11, BRA01 workstations.	Application & Host Support MPLS VPN	Testing Teams file transfer to /from Infrastructure.	SFTP	115
SAS	Application Servers & Counters	Secure channel between SAS ssh client and target SSH Server.	ssh	22
SAS	Application servers	Server Support Teams, Application Support Teams and Testing Teams access to Infrastructure.	RDP*	3389

** Only in exceptional circumstances and only to DC hosted servers*

DNS will be used for name resolution. Each server in the BladeFrame has a single NIC and connectivity and resilience is provided using a virtual switch within the BladeFrame. See ARC/PPS/ARC/0001.

For INF-2 there will be one SAS (SSN01) in BladeFrame BF5.

Server Name	SSN01
VLAN	2696
IP address	172.17.200.149
Subnet Mask	255.255.255.0
Gateway	172.17.200.158

The remote sites will access IRE19 at INF-2 as follows:

BRA01	Support users will be routed across the corporate network connecting to the SAS Test counter terminals will be routed across the FSBN connecting to load balanced services in the Test Branch DMZ.
STE09	Support users will be routed across the corporate network connecting to the SAS.
IRE11	Support users will be routed across the corporate network connecting to the SAS.
WGN01	Support users will be routed across the corporate network connecting to the SAS.

Add Reference LAN and WAN design for INF2.

System Requirement - T-RSD-14

System Requirement - T-RSD-21

©Copyright Fujitsu Services Ltd 2007

POL00395680

7 Manageability

The SAS can be managed remotely using Terminal Server and access through the BladeFrame console.

Systems Management tool – Tivoli will provide remote control access to this server.

Command logger service, and critical Windows OS services should be monitored and alerted on.

General performance alerting should be carried out.

Provisioning of SAS, patching and software distribution will be provided by Tivoli Provisioning Manager (TPM).

©Copyright Fujitsu Services Ltd 2007

POL00395680

8 System Qualities

8.1 Security

The security of the SAS and the supported platforms it is used to access will be ensured by the features described in the following sub sections.

8.1.1 Role based access and Controlled Tasks

Support users roles will be defined in AD and in the Tivoli Management Framework. This will ensure that only selected users will have permission to carry out potentially hazardous tasks on target platforms. Tasks identified by SSC as repeatable and low risk will be passed to 2nd line support after development and testing.

8.1.2 Encrypted Communication

Refer to the OpenSSH, Cygwin, Sudosh high level design – document reference to be added.

8.1.3 Strong Authentication

See high level design for Strong Authentication - DES/SEC/HLD/0001. This provides Windows 2003 natively supported 2 factor authentication using USB tokens.

8.1.4 Windows Operating System

The Windows 2003 platform poa_bastian.xml security policy is applied. This is part of the platform foundation build and supplied in the windows distribution. Security patches relevant at the date of first build will be applied to the platform and these will be documented. All other patching will be subject to the patching and upgrade policies and processes.

RDP traffic from the remote support workstations and laptops to the SAS will be encrypted using 128 bit SSL. See DES/SEC/HLD/0003 - HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN for details of the Certificate server that would be required for this.

8.2 Availability

The platform will provide resilience and repair described in the Windows 2003 platform design. For the blade hosted SAS in IRE11 and IRE19.

For HNG-X it is planned to have 3 SAS in each Data Centre.

©Copyright Fujitsu Services Ltd 2007

POL00395680

8.3 Performance

See the Windows 2003 Platform design for details of how this platform meets performance requirements. In summary the base build has improved performance by increased page file size on a dedicated disk and optimised disk partition configuration.

To ensure adequate terminal server performance all third party products should be supported under the terminal server environment. Where suppliers do not specifically state support under terminal services, these products should be adequately tested to ensure they do not adversely affect the performance of the server.

8.4 Usability

The service has been designed on Microsoft Terminal Server. Although this provides a GUI for interactive use, the system will not be used interactively except for SAS platform set up and maintenance. Users from SSC, SMG and ISD, will log on through the Terminal Server Client on the local Support Workstation, and be given access through ssh, client software and through the Terminal Server profile to the target system, applications or files.

8.5 Potential for Change

The focus of ssh session logging may be moved from the client to the ssh server service removing the need for the command logger on the SAS. Sudosh may be used to log ssh session content to the syslog file which would then be picked up by the audit solution.

Additional support tools and clients may be installed on the SAS in future. These clients must ensure that they have adequate, secure auditing or that application auditing takes place at the application server.

Additional SAS can be added if additional support users or support groups require access to the HNG-X infrastructure.

©Copyright Fujitsu Services Ltd 2007

POL00395680

9 Implementation

The SAS build is provisioned using the scripted Standard Windows 2003 build. Additional tasks to complete the build are:

- Disk Configuration
- Configuration of Terminal Server and licensing
- Delivery of common component packages
- Installation of packaged applications

Refer to DES/PPS/PPD/0005 - Platform Physical Design For Secure Access Server - INF2.

POL00395680

10 Application Development

Refer to the OpenSSH, Cygwin, Sudosh high level design

©Copyright Fujitsu Services Ltd 2007

POL00395680

11 Testing and Validation

Operational proofing will be carried out by the ISD team in Belfast to ensure that all required systems are accessible remotely.

For details of INF-2 Infrastructure testing refer to TST/SYT/HTP/0005 – HNG-X System Test (Infrastructure) High Level Test Plan.

POL00395680

12 Risks and Assumptions

The following risks and assumptions have been identified with the SAS design for HNG-X:

Risks:

- Delays due to licences for TS CALs will limit access.
- ssh command auditing solution not developed in time.
- Security not tight enough enabling changes to be made to the SAS

Assumptions:

- Assumed that there will be a level of auditing on supported DC servers accessed using specific clients.
- Assumed that development will take place with the installed version of cygwin. If a later version is released prior to development the version of cygwin used for INF-2 will be replaced.
- Support skills are available to support the open source code that is compiled and release as part of this design.

©Copyright Fujitsu Services Ltd 2007

POL00395680

©Copyright Fujitsu Services Ltd 2007

POL00395680

13 Requirements Traceability

For the full requirements Traceability Matrix for Remote Support & Diagnostics select the link below.

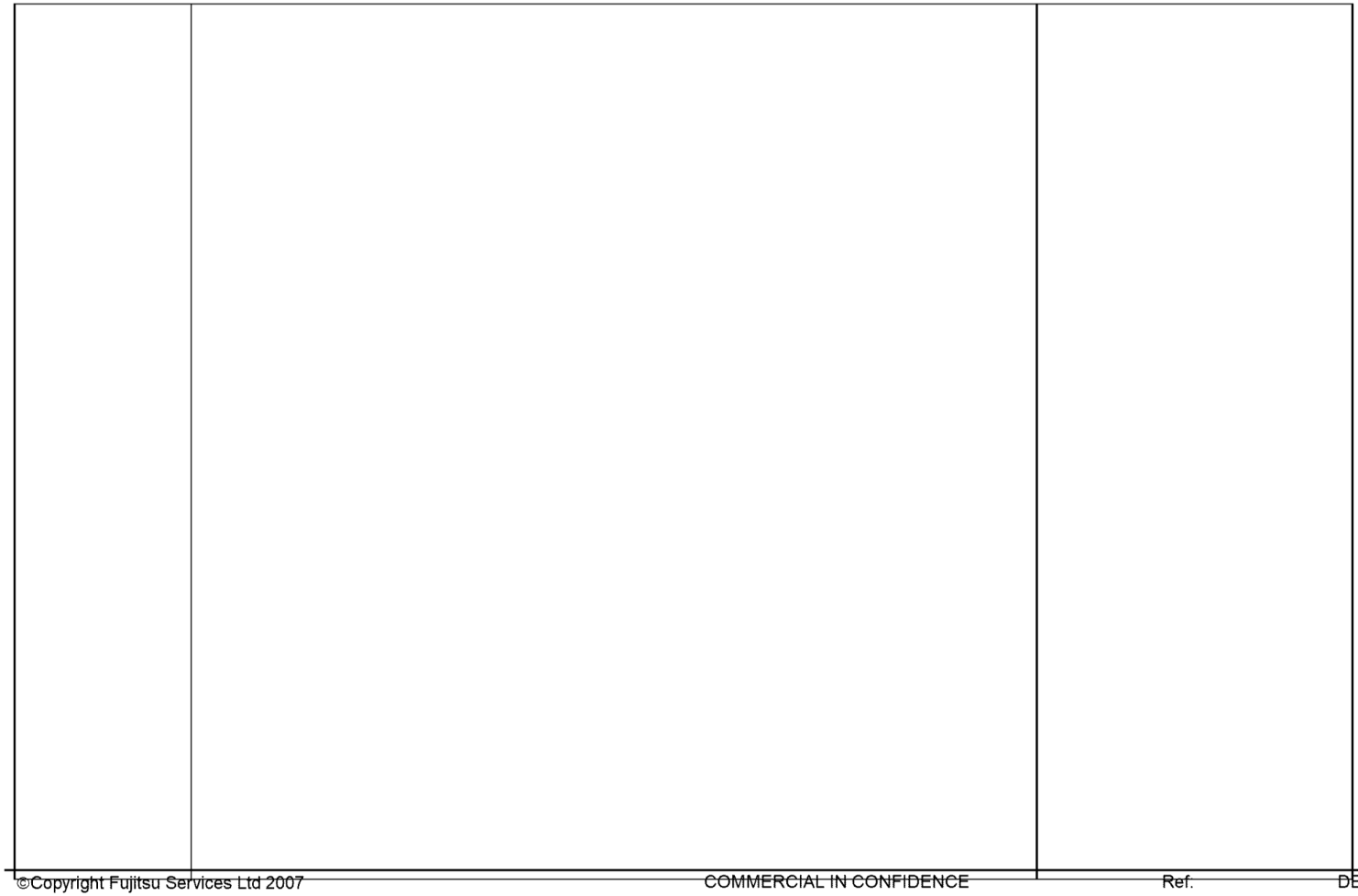
Sys Reqs for Remote Support and Diagnost

Table 1 - SAS System Requirements – provides a summary of the systems requirements that apply to this HLD.

SRS Ref.	System Requirement	HLD Section Ref.
T-RSD-1	Fully logged and auditable Open Secure Shell or Open SSH facilities shall be provided for 2nd and 3rd line support staff.	4.1.2 - Audit 4.3.2 - OpenSSH
T-RSD-2	Logged and auditable support access to management servers should be provided using web based clients, installed client software or shh. (e.g. ACE SecurID server, Aurora, TMR)	4.3.6 - Web Clients 4.3.7 - EMC Client and Tools 4.3.8 - Microsoft SQL Server 2005 Management Studio SP2 4.3.9- Oracle 10g Client 4.3.11 - Tivoli Client and tools
T-RSD-3	Role based support access shall be provided to 2nd and 3rd line support staff.	4.1.1 - Access
T-RSD-4	A secure file transfer application with a windows style graphical interface shall be provided for the transfer of diagnostic logs and other selected evidence files.	**13.1.1 4.3.3 - BSEC**

©Copyright Fujitsu Services Ltd 2007

POL00395680



©Copyright Fujitsu Services Ltd 2007

POL00395680

T-RSD-5	The secure file transfer application should be one way only for SMC and 2 way for SSC.	**13.1.3 4.3.3 - BSEC** For establishing the true identity of the admin/support users authorised to access HNG-X platforms, at any SAS Servers for the HNG-X project, BSEC software is installed on all SAS servers. For details refer to DES/SEC/HLD/0001. **13.1.4 Branch Router Access** All Branch Routers are accessible from Headend device in the data center and there is network connection between SAS server and Headend device. Therefore Telnet/FTP connections to Brach Router are made from SAS server. As all communication is taking place through Headend device therefore a common

©Copyright Fujitsu Services Ltd 2007

POL00395680

		support userid and password will be used. **Secure File Transfer**
T-RSD-6	Directories accessible by the secure file transfer application should be subject to control.	**13.1.5 4.3.3 - BSEC** For establishing the true identity of the admin/support users authorised to access HNG-X platforms, at any SAS Servers for the HNG-X project, BSEC software is installed on all SAS servers. For details refer to DES/SEC/HLD/0001. **13.1.6 Branch Router Access** All Branch Routers are accessible from Headend device in the data center and there is network connection between SAS server and Headend device. Therefore Telnet/FTP connections to

©Copyright Fujitsu Services Ltd 2007

POL00395680

		Brach Router are made from SAS server. As all communication is taking place through Headend device therefore a common support userid and password will be used. **Secure File Transfer**
T-RSD-7	For the secure file transfer application all transfers and attempted transfers should be logged at the server so the GUI interface does not need to be recorded. It is expected that graphical logging will not be required as the graphical secure ftp tool should be run using ssh and can be logged at the server.	**13.1.7 4.3.3 - BSEC** For establishing the true identity of the admin/support users authorised to access HNG-X platforms, at any SAS Servers for the HNG-X project, BSEC software is installed on all SAS servers. For details refer to DES/SEC/HLD/0001. **13.1.8 Branch Router Access** All Branch Routers are accessible from Headend

POL00395680

		device in the data center and there is network connection between SAS server and Headend device. Therefore Telnet/FTP connections to Brach Router are made from SAS server. As all communication is taking place through Headend device therefore a common support userid and password will be used. **Secure File Transfer**
T-RSD-8	For the secure file transfer application all logs should be secure and be picked up by the audit solution.	**13.1.9 4.3.3 - BSEC** For establishing the true identity of the admin/support users authorised to access HNG-X platforms, at any SAS Servers for the HNG-X project, BSEC software is installed on all SAS servers. For details refer to DES/SEC/HLD/0001. **13.1.10 Branch**

POL00395680

		13.1.11 Router Access All Branch Routers are accessible from Headend device in the data center and there is network connection between SAS server and Headend device. Therefore Telnet/FTP connections to Brach Router are made from SAS server. As all communication is taking place through Headend device therefore a common support userid and password will be used. **Secure File Transfer**
T-RSD-9	Two factor authentication shall be used to control access to the Secure Access servers	4.1.1 - Access
T-RSD-10	Out of Hours support shall be provided using dedicated, standard secure laptops. These shall be password protected.	4.1.1 - Access
T-RSD-111	The OOH laptops shall have locked down configurations and minimal internet access (access should be provided to some intranet sites and web client access to support applications).	
T-RSD-12	OOH laptops should have the standard Fujitsu VPN solution, personal firewall, PGP and antivirus protection installed and should also incorporate a challenge/response procedure.	
T-RSD-13	OOH shall also provide access during disaster recovery situations.	4.1.1 - Access

©Copyright Fujitsu Services Ltd 2007

POL00395680

T-RSD-14	The standard Fujitsu Services VPN solution will be used to gain access to the Fujitsu corporate network	6 - Networks
T-RSD-15	OOH Laptops for 3rd line support should be able to access Support Workstations preferably by RDP. Support Workstations require access to BSDB, SAS and SSC Servers directly.	4.1.1 - Access 4.3.9- Oracle 10g Client
T-RSD-21	The dedicated workstations shall sit on the POA network and the non-dedicated workstations will access the support networks through the corporate VPN. Access to the remote support framework will be from the following type of user: · POA dedicated support staff · Non-dedicated Fujitsu support staff (working on several accounts)	6 - Networks
T-RSD-22	SSC Workstations should have direct access to Databases, SQL*Net and the Microsoft equivalent in order to perform custom diagnostics and for the development of bespoke interfaces. Access to BSDB, SSC Servers only.	4.1.1 - Access
T-RSD-29	All applications shall provide diagnostic or text files that can be self managed so that they do not consume disc space indefinitely. Log files should kept for a specified time period (the default being one week)	4.1.2 - Audit
T-RSD-30	All applications shall store log, audit and tracing files in a common, agreed location. The standard format of these files will be defined, agreed and documented.	4.1.2 - Audit
T-RSD-34	All services shall have the ability to be stopped and started by the management tools. Performance reporting metrics should also be defined for applications and reported to the appropriate management tools.	4.1.2 - Audit
T-RSD-35	The SSC shall be able to provoke a dump of the operating system in order to examine a problem in more detail. This would be compliant for counters under strictly controlled circumstances but not for DC servers. The dump would not be encrypted.	

Table 1 - SAS System Requirements

©Copyright Fujitsu Services Ltd 2007

POL00395680

©Copyright Fujitsu Services Ltd 2007

POL00395680

14 Appendix A – Windows 2003 Admin Tools

Horizon	W2K3 Tool	Description	W2K3 Support Tools	W2K3 Reskit Tools	MMC Snap-ins
COMPREG.EXE	?		acldiag.exe	adlb.exe	.NET Framework 1.1 Configuration
DRIVERS.EXE	driverquery	Displays a list of all installed device drivers and their properties.	addiag.exe	atmarp.exe	Active Directory Domains and Trusts
DUMPEL.EXE	?		apmstat.exe	atmlane.exe	Active Directory Sites and Services
GETMAC.EXE	getmac	Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.	bindiff.exe	autoexnt.exe	Active Diectory Users and Computers
GETSID.EXE	?		bitsadmin.exe	cdburn.exe	ActiveX Control
KILL.EXE	?		browstat.exe	cepsetup.exe	Authorization Manager
PSTAT.EXE	?		cabarc.exe	chklnks.exe	Certificate Templates
PULIST.EXE	?		dcdiag.exe	chknic.exe	Certificates
REG.EXE	reg	Performs add, change, import, export and other operations on registry subkey information and values in registry entries. reg add, reg compare, reg copy, reg delete, reg export, reg import, reg load, reg query, reg restore, reg save, reg unload	depends.exe	cleanspl.exe	Certification Authority
ROBOCOPY.EXE	Robocopy	in w2k3 reskit tools	devcon.exe	clearmem.exe	Component Services
SC.EXE	sc.exe	Communicates with the Service Controller and installed services. SC.exe retrieves and sets control information about services. You can use SC.exe sc boot, sc config, sc continue, sc control, sc create, sc delete, sc description, sc enumdepend, sc failure, sc getdisplayname, sc getkeyname, sc interrogate, sc lock, sc pause, sc qc, sc qdescription, sc qfailure, sc query, sc queryex, sc querylock, sc sdset, sc sdshow, sc start, sc stop	dfsutil.exe	clusterrecovery.exe	Computer Management

©Copyright Fujitsu Services Ltd 2007

POL00395680

SCANREG.EXE	?		dhcploc.exe	compress.exe	Device Manager
SCLIST.EXE	?		diruse.exe	confdisk.exe	Disk Defragmenter
SCOPY.EXE	?		dmdiag.exe	consume.exe	Disk Management
SHOWACLS.EXE	showacls.exe	in w2k3 reskit tools	dnscmd.exe	creatfil.exe	Distributed File System
SHOWDISK.EXE	?		dnslint.exe	csccmd.exe	Event Viewer
SHOWGRPS.EXE	?		dsacls.exe	custreasonedit.exe	Folder
SHOWMBRS.EXE	?		dsastat.exe	delprof.exe	Group Policy Object Editor
SHUTDOWN.EXE	shutdown	Enables you to shut down or restart local or remote computers one at a time.	dskprobe.exe	dh.exe	Indexing Service
SLEEP.EXE	sleep.exe	in w2k3 reskit tools	efsinfo.exe	diskraid.exe	Internet Authentication Service
TLIST.EXE	tasklist	Displays a list of currently running processes on either a local or remote machine.	exctrlst.exe	diskuse.exe	IP Security Monitor
			filever.exe	dnsdiag.exe	IP Security Policy Management
			ftonline.exe	dvdburn.exe	Link to Web Address
			getsid.exe	empty.exe	Local Users and Groups
			gflags.exe	eventcombmt.exe	Performance Logs and ALerts
			httpcfg.exe	fcsetup.exe	Remote Desktops
			iasparse.exe	getcm.exe	Removable Storage Management
			ksetup.exe	gpmonitor.exe	Resultant Set of Policy
			ktpass.exe	gpotool.exe	Routing and Remote Access
			ldp.exe	hlscan.exe	Security Configuration and Analysis
			memsnap.exe	ifilttst.exe	Security Templates
			movetree.exe	ifmember.exe	Services
			msicuu.exe	iniman.exe	Shared Folders
			msizap.exe	instcm.exe	Telephony
			netcap.exe	instexnt.exe	Terminal Services Configuration
			netdiag.exe	instsrv.exe	Wireless Monitor
			netdom.exe	intfiltr.exe	WMI Control
			nltest.exe	kerbtray.exe	
			ntfrsutl.exe	kernrate.exe	
			poolmon.exe	klist.exe	
			portqry.exe	krt.exe	
			remote.exe	linkd.exe	

©Copyright Fujitsu Services Ltd 2007

POL00395680

			repadmin.exe	linkspeed.exe	
			replmon.exe	list.exe	
			rsdiag.exe	lockoutstatus.exe	
			rsdir.exe	logtime.exe	
			sdcheck.exe	lsreport.exe	
			setspn.exe	lsview.exe	
			showaccs.exe	mcast.exe	
			sidwalk.exe	memmonitor.exe	
			SPCheck.exe	memtriage.exe	
			windiff.exe	mibcc.exe	
			xcacls.exe	moveuser.exe	
				mqcast.exe	
				mqcatch.exe	
				nlsinfo.exe	
				now.exe	
				ntimer.exe	
				ntrights.exe	
				oh.exe	
				oleview.exe	
				pathman.exe	
				permcopy.exe	
				perms.exe	
				pfmon.exe	
				pmon.exe	
				printdriverinfo.exe	
				qgrep.exe	
				qtcp.exe	
				rassrvmon.exe	
				rcontrolad.exe	
				regini.exe	
				regview.exe	
				remapkey.exe	
				reportgen.exe	
				rktools.exe	

©Copyright Fujitsu Services Ltd 2007

POL00395680

				robocopy.exe	
				rpccfg.exe	
				rpcdump.exe	
				rpcping.exe	
				rpingc.exe	
				rpings.exe	
				rqc.exe	
				rqs.exe	
				setprinter.exe	
				showacls.exe	
				showperf.exe	
				showpriv.exe	
				sleep.exe	
				sonar.exe	
				splinfo.exe	
				srvany.exe	
				srvcheck.exe	
				srvinfo.exe	
				srvmgr.exe	
				ssdformat.exe	
				subinacl.exe	
				tail.exe	
				tccom.exe	
				tcmon.exe	
				timeit.exe	
				timezone.exe	
				tsctst.exe	
				tsscalling.exe	
				uddicatschemeeditor.exe	
				uddiconfig.exe	
				uddidataexport.exe	
				usrmgr.exe	
				vadump.exe	
				vfi.exe	

©Copyright Fujitsu Services Ltd 2007

POL00395680

				volperf.exe	
				volrest.exe	
				vrfydsk.exe	
				winhttpcertcfg.exe	
				winhttptracecfg.exe	
				winpolicies.exe	

©Copyright Fujitsu Services Ltd 2007