FUJ00089535

Document Title: Remote Support Secure Access Server High Level Design

Document Type: High Level Design (HLD)

Document Reference: DES/SYM/HLD/0017

Release: 15

Abstract: This document describes the High Level Design for the Remote Support Secure Access Server.

Document Status: APPROVED

Author & Dept: John Bradley

Internal Distribution:

External Distribution:

Approval Authorities:

Name	Role	Signature	Date
Gareth Jenkins	HDCR Solution Owner		

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

FUJ00089535

0 Document Control

0.1 Table of Contents

FUJ00089535

FUJ00089535

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 V1.1	
	19/12/2007	Document changed	
1.1	7/1/2008	Document	
2.0	22/04/08	FTP design for SSC is added. FTP Design changed due to changes in NW	
2.1	10/06/2009	Added POL-SAP requirements	
2.2	13/01/2016	Introduction of SSNv2 for HDCR	CP1560
2.3	20/01/2016	Added detail for Windows 2012 RDS	
2.4	22/02/2016	Included detail for iKey SSNV2 exception access and User Profile Disk share location	
2.5	1/4/2016	Review Comments	
3.0	24/10/2016	Approval version	

0.3 Review Details

(*) = Reviewers that returned comments

Review Comments by :	16-03-2016
Review Comments to :	John Bradley & PostOfficeAccountDocumentManagement@ GRO

Mandatory Review	
Role	***Name***
POA Chief Architect	Torstein Godeseth
POA Dev Architecture	Andrew Thomas(*)
POA Business Requirements and Architecture	Stephen Evans(*)
POA Development Management	Keith Tarran
POA Security Architecture	Dave Haywood
Solution Owner	Gareth Jenkins
HNS Networks Architect	Steve Freke
POA Test	Mark Ascott
POA SSC	Steve Parker/Phil Breakspear(*)
POA SSC	Mark Wright (SSCv2 Platform Owner)
POA HNS Senior Operations Manager	Alex Kemp(*)

FUJ00089535

Unix and Storage Team	Andrew Gibson(*)
Unix and Storage Team	Ed Ashford
Windows NT	Ryan Hawks
Optional Review	
Role	***Name***
POA Business Requirements and Architecture	Sarah Selwyn
POA Business Requirements and Architecture	Jon Hulme
POA Business Requirements and Architecture	Chris Bailey
POA Business Requirements and Architecture	Clare Keane
POA Development Management	Steve Goddard
POA Design and Development	Keith Hunt
POA Integration	Vijesh Pandya
POA Quality & Compliance Manager	Bill Membery
POA Test	Pete Dreweatt/Michael Welch(*)
POA Programme Manager	Brian McCann
POA Project Management	Geof Slocombe
POA Design and Development	Stuart Honey
POA Service Introduction Manager; BAS Lead SDM & Risk Manager	Yannis Symvoulidis
POA Release Management	Alan Flack
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	***Name***
POA Development Management	Iain Janssens
POA Sec Ops	Stephen Godfrey
POA BAS Senior Service Delivery Manager	Steve Bansal

(*) = 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			Remote Support and Diagnostics Topic Architecture	Dimensions
DES/PPS/HLD2743			Windows Server 2012 High Level Design for HNG-X	Dimensions

FUJ00089535

DES/PPS/HLD/0003			HNG-X Active Directory High Level Design	Dimensions
ARC/PPS/ARC/0001			HNG-X Platforms and Storage Architecture	Dimensions
DES/SEC/HLD/0001			HNG-X Strong Authentication High Level Design	Dimensions
DES/SEC/HLD/0003			HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN	Dimensions
DES/PPS/PPD/0005			Platform Physical Design For Secure Access Server - INF2	Dimensions
SY/SOD/009			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
DES/SYM/PPD/2977			SSNv2 Platform Physical 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
RDCB	Remote Desktop Connection Broker
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RDSH	Remote Desktop Session Host
SAS	Secure Access Server
SSNV2	Platform name of Secure Access Server for HNG-X
SFTP	Secure File Transfer Protocol
SMG	Systems Management Group
SSC	System Support Centre. 3rd Line support

FUJ00089535

SSH	Secure Shell
RDP CAL	Remote Desktop Client Access Licence
TEM	Tivoli Endpoint Manager

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.

0.7 Changes Expected

Changes
This HLD will be updated for HDCR release 16 and 17

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

FUJ00089535

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 workstations to the SAS (SSNv2), the applications and clients installed on the SAS (SSNv2) and the secure method used to connect to supported platforms.

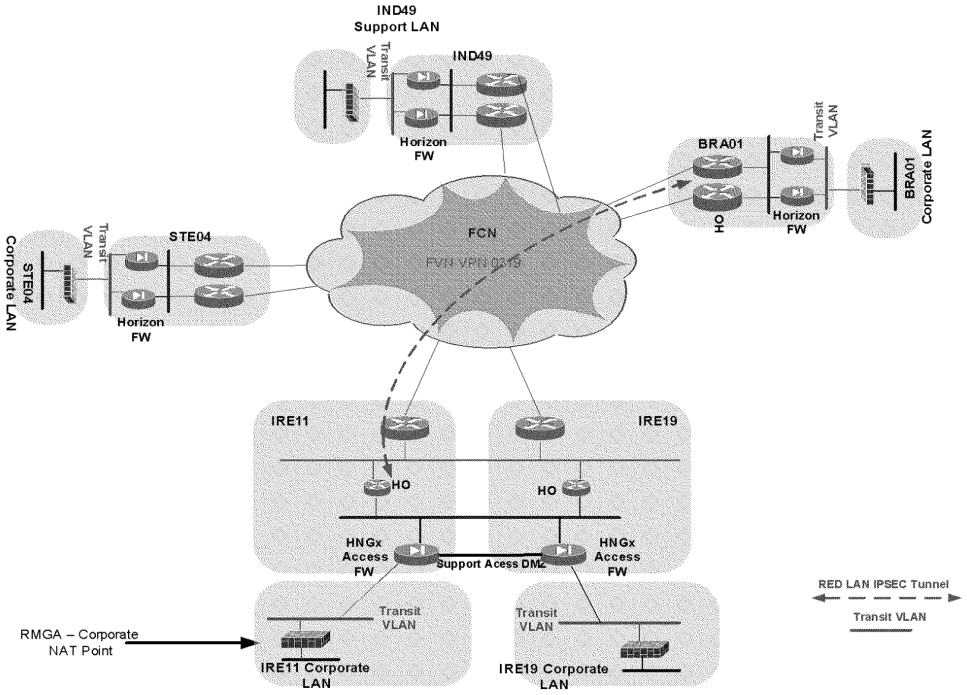
The support workstations and laptops used to connect to the SAS (SSNv2) are out of scope for this design.

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 (SSNv2) is described in ARC/SYS/ARC/0004. The diagram below shows where the SSNv2 fits into the overall support architecture. The SSNV2v1 will be retained to support legacy HNG/x platforms.

FUJ00089535



FUJ00089535

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 SSNv2 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.

FUJ00089535

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 SSNV2 to the managed operational platforms.
- Secure web based access to campus servers. All access to SSNv2 server will be on HTTPS (443) port. From SSNv2 onward to campus servers can be either on HTTPS or HTTP.
- Access to the System Management.

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

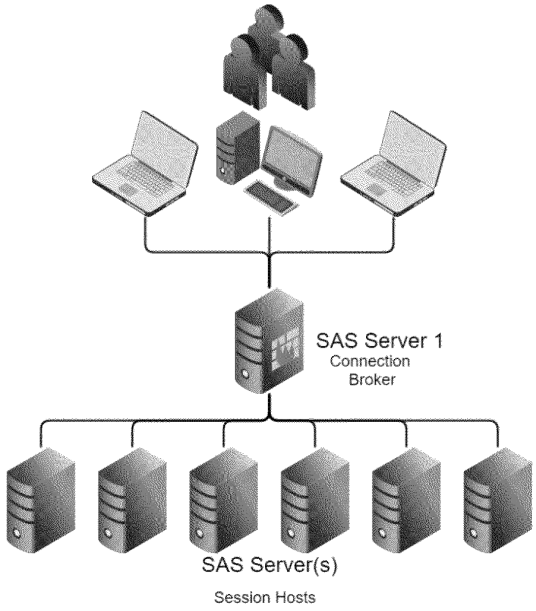
The aim of the Remote Support Secure Access Server HLD is to meet the requirements listed in **Table 1 - SAS (SSNV2) System Requirements**, in the Requirements Traceability Section of this document.

FUJ00089535

4 Sub-System Description

4.1 Secure Access Server Overview

The SSNv2 is based on the Microsoft Windows 2012 platform as described in DES/PPS/HLD2743 - Windows Server 2012 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 connect into the first SSNv2 which acts as a Connection Broker. The broker acts as a software load balancer, and assigns both a User Profile Drive and a Session Host for the user to connect to.

4.1.1 Access

The SAS (SSNv2) servers will be placed into a Remote Desktop Services deployment collection, and users will connect to the primary SAS (SSNv2) using the RDP client over SSL. The RDS deployment will enable multiple users to be connected to any of the SAS (SSNv2) collection. 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 (ref. DES/SEC/HLD/0001, DESSECHLD0004.DOC).

The two factor authentication system is provided by Safenet iKey software and USB dongle. The USB dongle will either be the iKey 4000 or the eTokens 5110 (TBC after compatibility testing)

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

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

FUJ00089535

A Secure Shell (ssh) client will be installed on the SAS (SSNV2) and ssh server will be installed on the operational platforms. This will provide a secure shell for support access.

Support workstations will access the SAS (SSNv2) collection over the Fujitsu Corporate Network using RDP.

A single SSNv2 server will be allocated as an 'exception' server, which will permit access to users who are unable to connect using their iKey. This server will be placed into its own collection inside of the Remote Desktop Services deployment, and will only permit access from users placed into the exception group in Active Directory, which is currently **ikey-exemptou-users**. Users attempting to access the exception SSNv2 will need to do so using its direct IP address, to ensure the connection broker does not attempt to push them onto an ikey-enabled SSNv2.

For the production environment, the SSNv2 Exception Server will be LPRPSSNV2203

4.1.2 Audit

Although no active command logging or keystroke logging is done, we are keeping the record of people logged on to SAS (SSNV2) server through double authentication and OS security policies for state servers. Security policy is implemented to raise alert when any file is copied or deleted to SAS (SSNV2) server. Also no user account is allowed to install any software on SAS (SSNv2). FTP folder will be maintained manually by SSC team.

All components of the SAS (SSNv2) 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.

4.1.3 Support and diagnostic tools

From the SAS (SSNv2) support users will be able to run the following support tools:

- Tivoli tasks
- Cygwin tools
- Installed software clients
- Web based clients
- Windows 2012 support tools
- RDP

4.2 Remote Desktop Services

Remote Desktop Services (RDS) is the modern version of Microsoft Terminal Services, and there are a few differences to the way RDS is configured.

An RDS system is known as a deployment, in this case a session-based desktop deployment will be used.

An RDS Deployment utilises the following server roles.

- Remote Desktop Connection Broker (RDCB). The connection broker role will be installed on the first SAS (SSNv2) and acts as the main connection point for clients. It then routes clients through to an available Session Host server (described below) and thus acts as a software load balancer.

FUJ00089535

- Remote Desktop Session Host (RDSH). The Remote Desktop Session Host role is the component that allows multiple users to log onto a server simultaneously (Windows Server nominally only otherwise allows two connections at most) and use applications on that server. The RDSH role will be installed on all the SAS (SSNV2's).
- Remote Desktop Licensing: This role is applied to a server in the deployment to provide licensing services. Each client accessing RDS requires a license. 'Per Device' licensing will be used.
- Remote Desktop Web Access: This role is installed as part of a deployment, but will not be utilised for the SAS (SSNV2) configuration.

Once the deployment is configured, a 'collection' is created under which the RDSH servers are assigned. A collection can provide access to RemoteApp software, but this will functionality will not be used, and instead the collection will purely be used to assign available RDSH servers for client connectivity and apply required configuration, for example User Profile Drives.

4.2.1 User Profiles

Remote Desktop Services in Windows 2012 gives the ability to use VHD virtual hard disk files as User Profile disks. These are accessible using UNC access to a Windows 2012 hosted file share. When a user logs into the SSNv2, a template VHD file is copied to a new file which matches the user's SID. This is then mapped transparently to the user, with the contents of their profile directory appearing as normal in Explorer, but being fully contained with the VHD file.

This enables full roaming profiles for a user, so no matter which SSNv2 they log in to, their profile is always accessible and kept in a central location. This also permits a more straightforward way of backing up user profiles, as only a single VHD file for each user will need to be backed up.

One disadvantage of using UPDs is that two RDS collections cannot use the same location for user profile files, so anyone connecting into the SSNv2 ikey Exception Server will not be able to access their normal roaming profile.

The user profile disks will be stored in a network share hosted by the SSCv2 server, lprpssc201.

For regular users, the share name will be NAS_SSNv2_USERS$, and for exception users, the share name will be NAS_SSNv2_IKEYEXCEPTIONS$

4.3 Administration Tools

4.3.1 Cygwin

Cygwin is installed as part of the standard Windows 2012 Member Server build.

This is detailed in the HLD for Windows 2012 DES/PPS/HLD/2743

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.

FUJ00089535

To establish an SSH session an SSH client is required on the SAS (SSNV2) and the SSH server service or daemon on the target system. The PuTTY OpenSSH client (PUTTY v0.66) will be used to connect from the SAS (SSNV2) to the ssh server. PuTTY also includes the command line tool PSCP which can be used to securely copy files between client and server.

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

System Requirement - T-RSD-1

4.3.3 Secure File Transfer

The COTS selected to provide SFTP to SSC is JScape. It will be installed on SSC server. For end to end file transfers all files will be transferred to SSC server and from there they will be pulled either to SSC workstation or to SAS (SSNV2) using PSCP client.

JSCAPE software is installed on SSC server, from SSC workstation files will be transferred to SSC server. Then user logged on to campus server via RDP / SSH session from SAS (SSNV2) will download files to campus server from SSC server. Similarly files will be pushed to SSC server from campus server and then using WSFTP client they will be downloaded to SSC workstation.

4.3.4 Web Clients

Microsoft Internet Explorer 11 and Mozilla Firefox will provide connection for web based clients. This access will not be audited on the SAS (SSNV2) and access should be restricted, secure and auditable on the target server. Web clients should use https and certificates will be provided by the Certificate Authority described in DES/SEC/HLD/0003 - HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN. For details please refer to DES/SEC/HLD/0003

System Requirement - T-RSD-2

4.3.5 Microsoft SQL Server 2014 Management Studio (SP1)

This provides management access to SQL Server databases.

System Requirement - T-RSD-2

Microsoft Virtual Server 2005 R2 SP1

4.3.6 Oracle 11g Client

The 11g client is proposed for a future release, R16.

System Requirement - T-RSD-2

System Requirement - T-RSD-22

4.3.7 JRE8 and JDK8

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. At this time, the version installed will be Java 8 64 bit.

Should any other version of Java be required for applications, it MUST be installed into its own custom directory, and programs relying on this other version must support being able to redirect to it, rather than the system default of Java 8.

FUJ00089535

4.1.8 BigFix Console

The BigFix console is the User Interface for the Big Fix application inetalled on the TEMv2 platform.

XWindow client

A client to provide a graphical user interface (GUI) for networked computers connecting to XServer application running on the server machine, through SSNV2 connection. The client will be installed on the SSNV2 servers and made available to remote human users when needed. Several XWindow client are available, on a free license basis, including Cygwin-X.

4.1.9 7-Zip

7-Zip is a multi-format archiver and unarchiver, compatible with all major formats of compression, including ZIP, RAR, BZIP and many more. It is freeware and has both GUI and command line interfaces.

4.1.10 Notepad++

Notepad++ is a freeware text-editor, with support for different file encodings (e.g. ANSI, UTF8) and different line-endings (e.g. Windows, Unix/Mac). It also provides regex search/replace functions, macros, and has a plugin system to allow for further customisation or ability.

4.1.11 Microsoft Office 2013

The version of Office 2013 to be installed on the SSNv2's should correspond to the version on corporate laptops. At the time of writing, this is Office Professional Plus 2013. Using the same version on both the server and support laptop ensures no extra licensing is required, although an initial license is needed to allow the software to be installed on the SSNv2 and activated.

FUJ00089535

5 Ireland Support Workstations (ISW)

Release 17 deliverable

5.1 Transfer of Evidence Files

Release 17 deliverable

FUJ00089535

6 Networks

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

Source	Destination	Description	Protocol	Ports
STE09, IRE11, BRA01 workstations.	SAS (SSNV2)	Server Support Teams, Application Support Teams and Testing Teams access SAS (SSNV2) and Test SAS (SSNV2).	RDP	3389
STE09, IRE11, BRA01 workstations.	Application & Host Support MPLS VPN	Testing Teams file transfer to /from Infrastructure.	SFTP	115
SAS (SSNV2)	Application Servers & Counters	Secure channel between SAS (SSNV2) ssh client and target SSH Server.	ssh	22
SAS (SSNv2)	Salesforce Servers	Secure channel between SAS (SSNV2) ssh client and target SSH Server.	ssh	22
SAS (SSNV2)	Application servers	Server Support Teams, Application Support Teams and Testing Teams access to Infrastructure.	RDP*	3389
SAS (SSNV2)	Application Servers	Oracle 10g access to all Oracle database servers		
SAS (SSNV2)	Application Servers	SQL server Management Studio		
SAS (SSNV2)	Microsoft Virtual Servers	Microsoft Virtual Server 2005 R2 SP1. This tool is used for the management virtual servers	TCP	1024
SSC	SAS (SSNV2)	This will provide access from SSC work station to SAS (SSNV2)	RDP, SFTP	3389 22
SAS (SSNV2)	BF11 blades: lprpr3d001 – SAP R/3 Database Server lprpr3d002 – SAP R/3 Database Server lprpr3d003 – SAP R/3 Database Server lprpxid001 – SAP XI Database Server lprpxid002 – SAP XI Database Server lprpxid003 – SAP XI	This will provide access for core SAP installs and XTTS work on the specified BF11 blades for member of the SAPAdmins group	TCP	22 for SSH, 21211-21219 for SAPInst GUI

FUJ00089535

	Database Server			

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

DNS will be used for name resolution. Each server in the BladeFrame server has virtual NIC and they are mapped to switch Blade, which has more than one NIC if required. Resilience is provided using a virtual switch within the BladeFrame. See ARC/PPS/ARC/0001.

The remote sites will access IRE Datacenters are as follows:

BRA01	Support users will be routed across the corporate network connecting to the SAS (SSNV2) 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 (SSNV2).
IRE11	Support users will be routed across the corporate network connecting to the SAS (SSNV2).
WAR08	Support users will be routed across the corporate network connecting to the SAS (SSNV2).
BLA01	Support users will be routed across the corporate network connecting to the SAS (SSNV2).

System Requirement - T-RSD-14

System Requirement - T-RSD-21

FUJ00089535

7 Manageability

The SAS (SSNV2) can be managed remotely using Remote Desktop and access through the BladeFrame console.

Systems Management tool – Tivoli will provide monitoring of this platform..

Critical Windows OS services should be monitored and alerted on. General performance alerting should be carried out. Provisioning of SAS (SSNV2), patching and software distribution will be provided by BigFix).

Refer to DESSYMHLD0004.doc for more details.

FUJ00089535

8 System Qualities

8.1 Security

The security of the SAS (SSNV2) 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 2012 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 (SSNV2) 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 (SSNV2) in IRE11 and IRE19.

For HNG-X it is planned to have 3 SAS (SSNV2) in each Data Centre.

FUJ00089535

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 (SSNV2) 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 (SSNV2). 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 (SSNV2) in future. These clients must ensure that they have adequate, secure auditing or that application auditing takes place at the application server.

Additional SAS (SSNV2) can be added if additional support users or support groups require access to the HNG-X infrastructure.

FUJ00089535

9 Implementation

The SAS (SSNV2) build is provisioned using the scripted Standard Windows 2012 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/2977 - Platform Physical Design For Secure Access Server – SSNv2

9.1 Installation Sequence

The installation sequence to create and configure the Remote Desktop Services deployment for the SSNV2's is as follows:

1. Windows 2012 base builds provisioned
2. Disk and Share setup
3. TEM-deployed PowerShell script to Windows 2012 member server. Script will create a Remote Desktop Services deployment, assigning appropriate roles and features to SSNv2 servers, rebooting as necessary to complete the installation. Collection will be created and SSNV2's added as RD Session Hosts to collection, permitting remote desktop access.
4. TEM-deployed PowerShell script to SSNv2 #1, to configure shared drive on H: to hold user profiles. RDS collection updated to point to this shared drive as User Profile Disk area.
5. TEM-deployed additional software to SSNv2's.

FUJ00089535

10 Application Development

Refer to the OpenSSH, Cygwin, Sudosh high level design

FUJ00089535

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.

FUJ00089535

12 Risks and Assumptions

The following risks and assumptions have been identified with the SAS (SSNV2) design for HNG-X:

Risks:

- Delays due to licences for RD CALs will limit access.

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.

FUJ00089535

FUJ00089535

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 (SSNV2) 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.	4.3.3 -
T-RSD-5	The secure file transfer application should be one way only for SMC and 2 way for SSC.	4.3.3 -
T-RSD-6	Directories accessible by the secure file transfer application should be subject to	4.3.3 -

FUJ00089535

	control.	
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.	4.3.3 -
T-RSD-8	For the secure file transfer application all logs should be secure and be picked up by the audit solution.	4.3.3 -
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
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 (SSNV2) 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

FUJ00089535

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 (SSNV2) System Requirements

FUJ00089535

FUJ00089535

14