Document Title: Platform Physical Design for the Secure Access Server

Document Type: Platform Physical Design Specification

Release: BI3

Abstract:

This document specifies the platform physical design for the Secure Access Server platform. Using Microsoft Terminal Server and SSH software, it provides a secure and auditable access mechanism between support groups and operational platforms. The support platforms will access the supported platforms through the Secure Access Server.

Document Status: APPROVED

Originator & Dept: Kristine Neiras – IPDU DA

Contributors:

Internal Distribution: **Pathway Library and Reviewers**

External Distribution: Internal distribution only

Approval Authorities: *(See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Ian Morrison	IPDU Manager		
Debbie Richardson	IPDU Integration and Test Manager		
Alan D'Alvarez	PTU Manager		

0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	26/9/02	Initial Draft	

0.2 Review Details

Review Comments by :	24/10/2002
Review Comments to :	Kristine Neiras

Mandatory Review Authority	Name
Chief Architect	TBD
Security Development Manager	Mark Ascott *
IPDU Security Design Authority	Peter Robinson
IPDU Resilience Design Authority	Simon Fawkes
Estate Management Manager	Colin Mills
Technical Integration and Test Manager	Debbie Richardson *
SSC Manager	Mik Peach *
PIT	Christian Rota
Optional Review / Issued for Information	
ASD Manager	Tony Drahota
ASD Security	Geoffrey Vane
ASD Systems Management	Glenn Stephens
Estate Management Development	Peter Lawrowitsch
Performance Design Authority	James Stinchcombe
Maestro Schedule Development	Andy Scott
Quality & Audit	Jan Holmes *
SMC	Ian Bowen

Core Services	Warren Welsh
IPDU Audit Design	Bryan Muir
IPDU Cryptography Design	Will Dawson Keith Simons
IPDU System Test	Chris Rayner

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
1 TD/ARC/001			Technical Environment Description	PVCS
2 TD/ARC/012			Technical Environment Implementation for Release 2	PVCS
3 RS/REQ/022			Secure Role Definitions for SECURENT Build	PVCS
4 NB/SDS/001			System Design Specification for the Network Banking Application.	PVCS
5 TD/SDS/001			System Design Specification for Network Banking Service Infrastructure Enhancements.	PVCS
6 NB/SDS/007			System Design Specification for Network Banking End-to-End Service	PVCS
7 NB/SDS/006			System Design Specification for Network Banking Commodity Products	PVCS
8 SY/SOD/009			Secure Support Systems Outline	PVCS
9 RS/DES/010			KMS HLD	PVCS
10 PA/TEM/001	7.0	2/4/02	Fujitsu Services Document Template	PVCS
11 RS/DES/082			Pathway Live Estate NT Server Names	PVCS

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

0.4 Abbreviations/Definitions

The following are any terms specifically included in this document.

0.4.1 Abbreviations

Abbreviation	Definition
ACDB	AutoConfiguration Database
ACF	AutoConfiguration File
APDU	Application Products Delivery Unit
ATE	Automatic Targeting Engine
BI3	Banking Increment 3 (stage 3 of the Network Banking Project)
BOC	Belfast Operations Centre
BSD	Berkley Software Design Inc
BSF	Boot Server File
CHAP	Challenge Handshake Authentication Protocol
CNIM	Counter Network Infrastructure Manager
COTS	Commercial Off The Software
CS	Pathway Customer Services
DCAK	Debit Card Service Audit Key, double length 3-DES symmetric key
DCP	Debit Card Project
DCS	Debit Card Service, changed to DCP
DMZ	De-militarised zone
EFTPoS	Electronic Funds Transfer at the Point Of Sale
FAD	Post Office Outlet unique identification number
GPL	GNU General Public License
IETF	Internet Engineering Task Force.
IPDU	Infrastructure Products Delivery Unit
ISD	Infrastructure Services Division
KMA	Key Management Application
MS	Microsoft
MSS	
NWB	Network Banking
OBC	Operational Business Change
OCMS	Outlet Change Management Service

OCP	Operational Change Proposal
OMDB	Operational Management Database (database at the heart of the Tivoli System)
PIN Pads	Touch button pads for keying in a customers Personal Identification Number (PIN) - required for Network Banking.
PKI	Public Key
POL	Post Office Ltd
PVCS	Product Version Control System
QoS	Quality of Service (for the network)
RDMC	Reference Data Management Centre
RMS	Riposte Message Store
SMC	Systems Management Centre
SMDB	Systems Management Database
SOD	System Outline Design
SAS	Secure Access Server see SAS
SSAS	Secure Support Access Server
SSC	Systems Support Centre
TID	Terminal Identifier (for EFTPoS)
TK	Traffic Key
TRC	Tivoli Remote Console
TS	Terminal Server
TSC	Terminal Server Client
TSS	Terminal Server Server
TWC	TeamWare Crypto. Product used on Pathway to encrypt file store
UAR	Unattended reboot
VNC	Visual Network Computing
VPN	Virtual Private Network

0.4.2 Definitions

Term	Definition
Cygwin	Cygwin is a UNIX environment for Windows. It consists of: a UNIX emulation layer providing substantial UNIX API functionality; a collection of tools which provide UNIX/Linux look and feel.

0.5 Changes in this Version

Version	Changes
1.0	Updates from reviews. Submitted for approval.

0.6 Changes Expected

Changes
Changes to the hardware and software requirements during integration.

0.7 Table of Contents

1.0 Introduction

1.1 Purpose

This document is the Platform Physical Design Specification for the Secure Access Server which provides a secure and auditable mechanism to those units that support the Horizon system. The document describes hardware and software contents for the platform. It is to be used in conjunction with the documents listed in section 0.3.

1.2 Readership

This document is intended for delivery unit personnel, and the support staff within Pathway and Core Services. It has been developed to give an overview of the platform design structure and the detailed contents of the specified platform. The intention is to enable developers to plan the development of new applications and to allow Core Services staff to support the platforms forming part of the Pathway solution. It also provides a list of those facilities included as part of the delivered solution, enabling formal Build and Validation of the release contents.

1.3 Scope

Ref1 provides an overall description of the program down to the level needed for each type of platform and its position within the system architecture. The detailed functions required as part of the specification of this platform are covered as part of [8].

Several items of information within this document have been extracted from reference [8].

1.3.1 Document Set

This document forms part of the set that defines Pathway's secure support environment. For further detail, the reader should refer to the documents in 0.3.

1.3.2 Contents

This document is organised as follows:

Section	*Contents*
Section 1	Introduces the document and its position within the document set.
Section 2	Gives an overview of the context within which secure support operates and a brief description of the architecture of secure support in terms of its hardware and software.
Section 3	Describes the hardware components and architecture
Section 4	Describes the software components and architecture
Section 5	Describes the security facilities and provides a summary of their operation.
Section 6	Describes resilience and recovery features.
Section 7	Describes the provisions for performing Audits in the server.
Section 8	Details the software contents in the form of tables of components – table 1 describing the COTS applications purchased specifically for use on this platform, and table 2 listing those applications developed internally.
Section 9	Describes the potential for change both to the hardware and software.
Section 10	Lists any Platform build special requirements
Section 11	Describes the platform migration requirements (if any) and the method by which they will be achieved.
Section 12	Describes any platform inter-working dependencies.
Appendix	After Approval, where change applies only to components and not to the body of the document, eg version upgrade or additional WP, only the Appendix A and B will be circulated for comment and information.
Appendix A	Specific configuration detail.
Appendix B	Component changes for specific releases.

2.0 Overview

This section provides an overview of the design of secure support and the context in which it operates.

2.1 Business Context

Full details of the business context of the entire Horizon project are defined in [1]. This platform enhances the security and audit on support tasks required for the new Network Banking Service and Debit Card System at BI3 and S30.

The introduction of this platform will overcome some of the security issues that have been under manual control, and so at risk from deliberate or unintentional actions by support staff. As a result of the lack of access restriction and audit by the support groups, there is the opportunity to perpetrate fraud and to make changes to the operational systems that will impact on the integrity, resilience and security of the systems and their data.

2.2 Technical Context

The documents in section 0.3 provide the technical context. Two platforms are present on each campus site. There are three main issues resolved in this platform.

- Control access to operational platforms
- Audit access and changes
- Give remote access to tool sets on the operational platform

2.2.1 Access

All access to operational platforms will be controlled through the Secure Access Server. This is built using the Microsoft Windows 2000 system software which includes the Terminal Server products which monitor and restrict access to authorised roles with passwords from authorised platforms. The Secure Shell software (SSH) is present as a client on the Secure Access Server, affording access between the SSH servers on the operational platforms and the SSH clients on the support terminals.

2.2.2 Audit

All transactions conducted through the Secure Access Server are audited. A command logging service will create the audit logs in a predefined file. This data will be collected by the Audit system and from a known file.

2.2.3 Tool sets

Tool sets to manipulate the data and systems on the operational platforms is being provided by work packages to the SSH clients on those platforms and the support workstations. The active product on the SAS is a mechanism to allow the support users access to operational platforms.

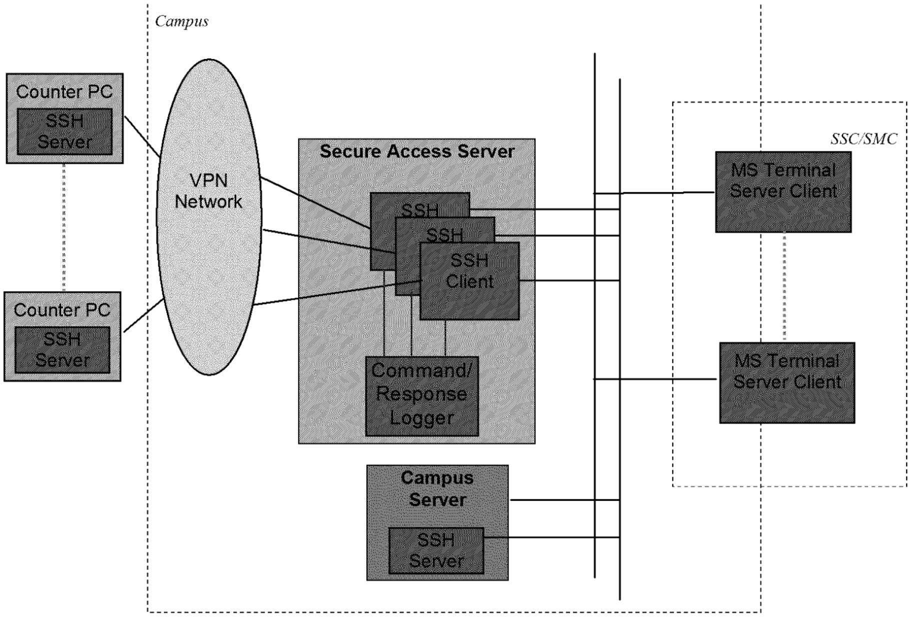
2.3 Design Principles

The general design principles intended for deployment in all platforms, is the maximum re-use of existing hardware platforms when software upgrades are required. It is an intention that minimal new software shall be designed and written – maximum use of existing COTS applications shall be made. In order to assist the production of the integration of COTS applications and the ready production of what few applications are required, the Horizon system will by default, look to use applications written for use with Microsoft NT4.0, SP6a. Use of UNIX operating system and applications will be minimised.

In order to provide a more resilient system, the Windows 2000 operating system has been chosen for the SAS platform. The facilities provided are limited to the SAS platform and all other platforms remain at their current operating system.

2.4 Overview of SAS Architecture

Ref [1] contains a detailed description of the entire Horizon architecture. Ref [8] provides the Secure Support System outline.



3.0 Hardware

3.1 Overview

The Fujitsu Primergy provides the base Secure Access Server platform. For resilience there are 2 SAS platforms at each campus site, in a separate security domain, accessed over the Pathway LAN. The SAS acts as a secure an auditable router between the support units and the operational platforms.

3.1.1 External Certification

All hardware used on the Horizon project is certified by the suppliers, to be conformant to EN54014 as indicated by the presence of a "CE" mark. All platforms used shall be specified as Validated to meet the requirement of Microsoft, and shall be listed in Microsoft's HCL.

3.2 Hardware Inventory

Machine Name	Fujitsu-Siemens Primergy F250 BU RH XEON Server
Manufacturer	Fujitsu-Siemens
Reference No.	S26361-K644-V302
Processor/Speed	XEON DP Processor 1.8GHz
No. Of Processors	1
Memory fitted	512kb
LAN controller	Intel 10/100
SCSI controller	
Fast-IDE controller	On-board Fast-IDE(ATA) controller for 2 x2 drives
Hard Disc	36GB,10k, U160,hot plug, 1"
Graphics controller	On-board PCI graphics ATI 8Mb
PCI slots	
CD-ROM/Writer	CD-ROM, ATAPI
Floppy Disc	Option S26361-F2575-E1

3.2.1 Extra Hardware Items

Quantity	Description	Reference No.	Manufacturer
1	RAID ctrl, 1x U160 int/ext, 32Mb Adaptec 2100S	S26361-F2405-E32	Fujitsu-Siemens
1	Fast Ethernet 10/100TX 2 port IPsec	S26361-F2643-E1	Fujitsu-Siemens
1	Hard Disc 36GB,10k, U160,hot plug, 1"	SNP:SY-F2336E136-P	Fujitsu-Siemens
1	Flexi-bay Option FD	S26361-F2575-E1	Fujitsu-Siemens
1	Power Supply Upgrade 400W(hot plug)	S26113-F453-E10	Fujitsu-Siemens
1	Mounting kit 19" FSC racks f.F2x0/Hxx0	S26361-F2734-E30	Fujitsu-Siemens

1	Fans upgrade kit hot-plug redundant	S26361-F2544-E1	Fujitsu-Siemens
2	1Gb DDR-RAM PC 1600 ECC	S26361-F2550-E524	Fujitsu-Siemens

3.3 Software Interfaces

3.3.1 Driver Software

Device	Filename	Version No.	Comment
TBD			As required

4.0 Software

4.1 Overview

Ref1 provides the complete picture of the entire Horizon architecture, including the software content. The architecture of the Secure Access Server environment is shown below.

The platform base software is Windows 2000. This supports the Terminal Server provided as part of the Windows 2000 Server software. The Open Secure Shell or OpenSSH facilities are provided by the COTS product which has been customised for Pathway's use as part of the CYGWIN environment. The platform security will be based on an enhanced version of Secure NT Secure build and include Tivoli, Triage and Athene Acquire.

Terminal Server is a product that can be configured to provide comprehensive access or denial options. It can be used to allow and deny access at specific times, by specific users, roles and through specific platforms and sub-nets to files, discs, platforms and devices. Some of these features will be used to support access between the support workstations and the operational platforms. The Command Logger will log all access and commands for future use by the Audit system.

Each campus will have 2 Secure Access Servers, built to the same specification.

5.0 Security Facilities

5.1 Encryption Software

No KMS keys will be used. TeamWARE Crypto is not used on the platform.

5.2 Windows Operating System

This platform is built with Windows 2000 Server with Service Pack 2 plus security hot-fixes.

5.3 Communications

All communication is through the Campus 100Mbit LAN.

5.4 Usability Features

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 the SSH, and through the Terminal Server profile to the target system, application or file.

The system has system management requirements limited to support for Tivoli, which will be used to download new versions of the software and to monitor the Application Event Log (which is used as the system audit trail). It also provides a command logger file for use by the Audit Server.

6.0 Resilience and Recovery Features

6.1 Hardware Resilience

Two Secure Access Servers are available on each Campus. There are no specific resilience features built into the systems.

7.0 Audit Provision

7.1 File/Object Auditing

This platform is designed to provide Audit information on access by support personnel to the operational platforms. Command Logger will provide the files for the Audit Server to retrieve.

Tivoli events will be raised.

NB The event log production will correspond to the Windows 2000 system implementation not the Windows NT4 implementation. As events are automatically logged to Tivoli, the Event Logs will be cycled as in the standard server builds.

8.0 Platform Component Structure

8.1 Platform Software Parts List [1]

[1] The tools/applications identified in this list have been sourced from the AS/REP/002 SY/SOD/009.

Part Name	Version	Supplier	Dependency
Tivoli		IBM	Licence required
Tivoli Generic Service Monitor			TBD may not work with Windows 2000
Tivoli Desktop	3.7	IBM	
Tec Java Console	3.7.1	IBM	
MANTOOLS			TBD may not work with Windows 2000
MANEVENT Filter Server			TBD may not work with Windows 2000
MANNTEP			TBD may not work with Windows 2000
ServerView		Fujitsu Siemens	Delivered with Server
ServerStart		Fujitsu Siemens	Delivered with Server
Generic 2000 Platform install routines		PIT	New for 2000
Admin Tools including Adminpak (partial), Browmon, Dommon, Netdom		Microsoft	
Internet Explorer	5.5	Microsoft	
Windows 2000 Server	SP2	Microsoft	Licence with server purchase
Windows 2000 Terminal Server		Microsoft	Licence with server purchase Config parameter
SecureNT		PIT	
Default File Security		PIT	
Support tools – Resource Kit		PIT	
Support tools -CYGWIN		IPDU Estate Management	
Common File Set		IPDU	
W2K Common File Set		IPDU	Under development
SSH Client		GNU –customised by IPDU Estate Management	Freeware SY/SOD/009

SSH Server W2K		GNU –customised by IPDU Estate Management	
Command Logger Service		IPDU Estate Management	
Oracle Client Tools for FJ Primergy	7.3	Oracle	Different to Compaq
Seagate Backup Exec Admin Interface	7.3	Seagate	
Support Tools WP		IPDU	
Triage Client	3.1	Metaquest	Licensed
Athene Acquire	7.30	Metron	Global Licence

8.2 PVCS Parts

The structure is defined down to, but not including the level of individual files that make up the platform; maintenance of the file level structure is the responsibility of the relevant development teams.

9.0 Potential for Change

Potential for change is a measure of the ability of the Platform Service to adapt to changing requirements or to new technology. This platform is currently being developed.

The following sections describe the facilities for changes to:

- Hardware
- System Software
- Third Party Product Software
- Applications Software

9.1 Hardware Enhancement

This is a new platform and changes may arise during integration. Hardware purchases have been made to cover the life of the hardware, to protect against changes in manufacture.

Hardware enhancements will only be permitted under rigid Change Control processes, following approval by the CCB. This includes all changes, whether they are to provide additional functionality or improved performance. The design aim is to minimise all such changes.

9.2 System Software Enhancement

The software is aimed to be released at S30. Changes may occur in the development and integration phases. Any future enhancements will be the subject of formal Change Proposal, approved by the CCB in the normal way.

9.3 Third Party Product Software Enhancement

The software is aimed to be released at S30. Changes may occur in the development and integration phases of the Retail Logic products and other product software which could be accommodated within the development plans. Any other changes or future enhancements will be the subject of formal Change Proposal, approved by the CCB in the normal way.

9.4 Application Software Enhancement

The software is aimed to be released at S30. Changes may occur in the development and integration phases of the Retail Logic Products and other product software which could be accommodated within the development plans. Any other changes or future enhancements will be the subject of formal Change Proposal, approved by the CCB in the normal way.

10.0 Platform Build

This is one of the first Windows2000 implementations. Also the platform is a new server type which will require some specific build, configuration and integration scripts. An initial build has been produced and this will be enhanced as development progresses.

11.0 Platform Migration

This is a new platform at S30. Initial software delivery and the upgrading of software will be carried out using the Tivoli System Management services.

12.0 Platform Inter-working dependencies

Each of the servers has a dual port NIC. This enables the connections to the local and the remote Campus LAN.

Where there is no change to the body of the document, system concept or interaction with other platforms the changes to components, only the Appendixes showing the changes will be circulated for information and review.

Appendix 1

This section will be to capture any specific usage or configuration detail. It is hoped that the reviewers will define what would be useful, eg port configs, share names, file names for standard or static files.

Operational Service

Configuration details

TBD

Disc configuration

C:

D:

TBD

Shares

C = system disc

Support tools

D = Pathway Applications

Terminal Server user profiles

Audit Logs

Command Logs

TBD

Appendix 2

Changes rel S30

Part Name	Version	Supplier	Dependency
Tivoli		IBM	Licence required
Tivoli Generic Service Monitor			TBD may not work with Windows 2000
Tivoli Desktop	3.7	IBM	
Tec Java Console	3.7.1	IBM	
MANTOOLS			TBD may not work with Windows 2000
MANEVENT Filter Server			TBD may not work with Windows 2000
MANNTEP			TBD may not work with Windows 2000
ServerView		Fujitsu Siemens	Delivered with Server
ServerStart		Fujitsu Siemens	Delivered with Server
Generic 2000 Platform install routines		PIT	New for 2000
Admin Tools including Adminpak (partial), Browmon, Dommon, Netdom		Microsoft	
Internet Explorer	5.5	Microsoft	
Windows 2000 Server	SP2	Microsoft	Licence with server purchase
Windows 2000 Terminal Server		Microsoft	Licence with server purchase Config parameter
SecureNT		PIT	
Default File Security		PIT	
Support tools – Resource		PIT	

Kit			
Support tools -CYGWIN		IPDU Estate Management	

Common File Set		IPDU	
W2K Common File Set		IPDU	Under development
SSH Client		GNU –customised by IPDU Estate Management	Freeware SY/SOD/009
SSH Server W2K		GNU –customised by IPDU Estate Management	
Command Logger Service		IPDU Estate Management	
Oracle Client Tools for FJ Primergy	7.3	Oracle	Different to Compaq
Seagate Backup Exec Admin Interface	7.3	Seagate	
Support Tools WP		IPDU	
Triage Client	3.1	Metaquest	Licensed
Athene Acquire	7.30	Metron	Global Licence
Part Name	Version	Supplier	Dependency
Tivoli		IBM	Licence required
Tivoli Generic Service Monitor			
TeamWARE Crypto	4.0		Licence required
ServerView		Fujitsu Siemens	
ServerStart		Fujitsu Siemens	
Generic 2000 Platform install routines			New for 2000?
Windows 2000 Server	SP2	Microsoft	Licence with server purchase
Windows 2000 Terminal Server		Microsoft	Licence with server purchase
SecureNT		PIT	
Default File Security		PIT	
Supporttools		PIT	TBD
Common File Set		IPDU	
W2K Common File Set		IPDU	
SSH Client		GNU –customised by	Freeware

		IPDU	
TBD			
Support Tools WP		IPDU	
Time Service	5.00.1399.1	Microsoft	Licence with server
Webtrends Security Analyser Client	4.1	Webtrends	
Triage Client	3.2	Metaquest	Licensed
Athene Acquire	7.30	Metron	Global Licence