FUJ00088036

Document Title: Secure Support System Outline Design

Document Type: System Outline Design

Release: BI3 S30

Abstract: This document describes the requirements and outline design for secure operational support access to Counters and Servers. The design is based on modifying the OpenSSH product to provide a command logging facility, these logs being maintained for audit purposes.

Document Status: **APPROVED**

Originator & Dept: Peter J Robinson — IPDU Security
Simon Fawkes — IPDU Service Management & Availability
Colin Mills — IPDU Estate Management

Contributors: Peter J Robinson — IPDU Security
Simon Fawkes — IPDU Service Management & Availability
Colin Mills — IPDU Estate Management

Internal Distribution See section 0.2

External Distribution None

Comments To: Originators

Approval Authorities (See PA/PRO/010 for Approval Roles)

Name	Position	Signature	Date
Ian Morrison	IPDU Delivery Manager		
Tony Drahota	ASD Manager		
Gill Jackson	Development Director		
Mike Deverell	PTU Manager		
Geoffrey Vane	Security TDA		
Mik Peach	SSC Manager		

FUJ00088036

0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	05/07/2002	Initial draft for review	CP3283
1.0	02/08/2002	First approved version taking into account comments on V0.1	CP3283

0.2 Review Details

See Review Role Matrix in PA/PRO/010 - ICL Pathway Document Management & Control Process, V8.0

Mandatory Review Authority	Name
IPDU Delivery Manager	Ian Morrison
ASD Manager	Tony Drahota
Development Director	Gill Jackson
PTU Manager	Mike Deverell
Security TDA	Geoffrey Vane
SSC Manager	Mik Peach
SSC System Specialist	Steve Parker
Optional Review / Issued for Information	
Colin Mills	Ian Bowen
Keith Hunt	Simon Fawkes
Peter Lawrowitsch	Glenn Stephens
David Tanner	George Zolkiewka
James Stinchcombe	Geoff Vane
Debbie Richardson	Karen Morley
Peter Wiles	Warren Welsh

0.3 Associated Documents

XRef	Reference	Version	Date	Title	Source
[CSREQ]	SY/REQ/001	0.2		Counter Support Requirements	PVCS
[CSSOD]	SY/SOD/001	0.2		Outline design for support migration from correspondence servers	PVCS
[KMFPS]	TSC/CRY/1067			File Protection for Debit Card Service	Crypto Team
[KMHLD]	RES/DES/010	7.0		Key Management High	PVCS

FUJ00088036

				Level Design[1]	
[NBSRI]	N/A	0.4	N/A	Network Banking Support Related Security Issues	S Fawkes
[NBSSH]	N/A	N/A	N/A	Support Access to NT systems in POs (and other NT systems)	P Boyd
[NBTST]	SY/SOD/006			Network Banking – Tivoli Based support Tasks	PVCS
[OSSH]	ISBN 0569000111	First Ed	2001	SSH, The Secure Shell. The definitive Guide	O'Reilly & Associates
[SFS]	RS/FSP/001			Security Functional Specification	PVCS
[SSH]	N/A	2.0		IETF SECSH	External

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

[1] Note V7.0 is in preparation and will cover DCS Crypto facilities including management and use of 3-DES keys such as DCAK.

FUJ00088036

0.4 Abbreviations/Definitions

The following abbreviations may have been used in this document.

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
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 see GNU GPL
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)

FUJ00088036

Abbreviation	Definition
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
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

0.5 Terminology.

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. See Cygwin.

0.6 Changes in this Version

Version	Changes

FUJ00088036

Version	Changes
0.1	First draft for comment
1.0	• Incorporatedcomments on V0.1. • Removal of all references to KMS keys, TeamWare Crypto etc. • Command lists added. • SSH Configuration values supplied. • Performance and sizing details addes. • Migration strategy added. • Testing strategy added. • Modifications to command log records.

0.7 Changes Expected

Changes
The following changes are expected: ➢ ISD are to confirm toolset requirements, purpose and modes of use (are ISD to install packages by this route, i.e. non Tivoli wrapped??). ➢ The following points non-Estate Management activities need to be agreed with the staff/teams identified, see 5.2.4.

FUJ00088036

0.8 Table of Contents

FUJ00088036

FUJ00088036

1.0 Introduction

1.1.1 General

[SFS] mandates the use of Tivoli Remote Console (TRC) for the remote administration of Data Centre platforms. This records an auditable trail of log-ins to all boxes accessed by the user. It is a matter of considerable discussion and correspondence that TRC is slow and difficult to administer. This has lead over time to BOC personnel relying heavily on the use of unauthorised tools (predominantly Rclient) to remotely administer the live estate. Its use is fundamental for the checking of errors. The tool does not however record individual user access to systems but simply record events[2] on the remote box that Administrator access has been used. No other information is provided including success/fail so it is not possible to simply audit failures. The use of such techniques puts Pathway in contravention of contractual undertakings to the Post Office. After the proposals in this SOD have been implemented a CP will be raised to phase out TRC (or limit its use to exceptional situations).

This document provides an outline design, which primarily stops Pathway being in contravention of its contractual undertakings but also provides an acceptable and agreed level of secure access to systems for support activities.

The design uses the facilities provided by the Secure Shell Protocol to provide secure, limited and audited command line access to any counter system in the Pathway network. SSH is a non- proprietary protocol defined by the IETF SECSH (see [SSH]). Being a non-proprietary protocol means that a number of ISVs provide products conforming to the standard, which can be interworked. Increased choice of supplier and potential consequential savings to Pathway may result which are not afforded by a "monoculture" solution; this may be an important factor when considering a solution for the Pathway estate which has 40,000+ managed PCs and servers.

[2] The event information is even then severely limited, (2002 info, 2004 warning and 2006 error).

FUJ00088036

1.2 Documentation

Documents relating to this System Outline Design are defined in Figure 1.

Additional documentation on the Secure Shell is available in [OSSH].

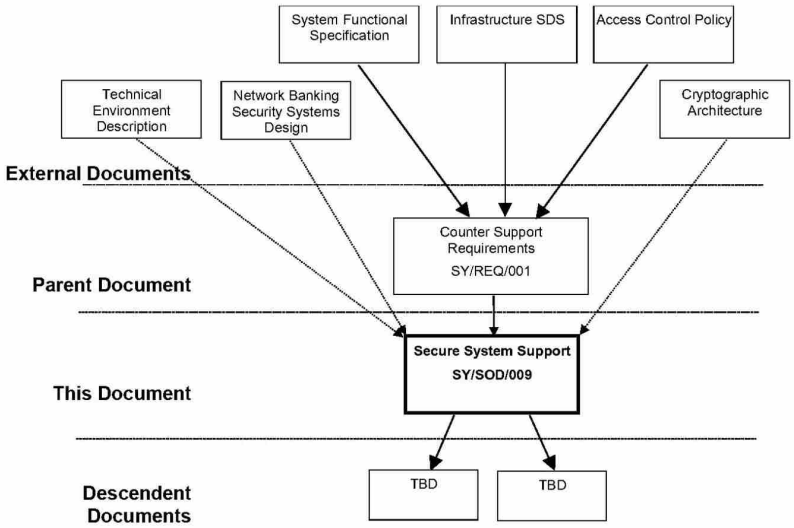

Figure 1: Relationship to other documents

FUJ00088036

2.0 Scope

2.1 In Scope

The scope of this design is not intended to address the full set of support requirements as defined in [CSREQ]. It is also not limited to just the areas identified within the design document, rather aims to address other security related issues with the current support practices, for example the un-audited insertion of code onto the live system in order to diagnose faults.

This document is intended to formally develop both the requirements and the solution for Counter Support Requirements as specified in [CSREQ].

The requirements for secure support are not explicitly stated in [CSREQ] however a number of the requirements are dependent on the provision of such a facility. This document identifies the requirements for such a facility and proposes a design, which will satisfy them.

2.2 Out of Scope

Full set of requirements defined in [CSREQ].

The future use of Tivoli Remote Console is out of scope of this document.

FUJ00088036

3.0 Design Principles

3.1 Principles

This System Outline Design is also based on the material resulting from the statements and investigations as documented in [NBSRI] and [NBSSH].

The major design principle is to use the Secure Shell (SSH) as the connection method between support staff and the counters and campus servers they have to administer. SSH is a non- proprietary protocol defined by the IETF SECSH (see [SSH]). Various implementations of SSH are available both commercial and open source. The design is based on the use of an open source version of SSH available from OpenSSH (see www.openssh.org). This product was chosen since one of the design principles is to facilitate security by logging all commands run when administering counters and servers. Whilst a command logging facility is available in certain SSH products (viz www.openssh.com) most have the draw back that they are end user configurable, i.e. can be turned off or on as they decide. However to facilitate security, ALL commands[3] have to be logged and end user control of such an option has to be removed. By using the OpenSSH.org product access to the source code is obtained and hence it can be tailored exactly to our requirements.

3.2 Assumptions

It is assumed that:

- Microsoft Terminal Server will be the host platform for establishing connections to managed clients;
- encrypted connections between the Campus and Counters although not required as this is provided by VPN will still be provided by SSH (this is a property of the client server connection it establishes);
- intra Campus connections will be also be encrypted, as per above;
- support of OpenSSH will be undertaken entirely from within Pathway;
- a 'single point of failure' resilience strategy will be acceptable, in particular to the SSC.

[3] Terms such as "commands" and "command logger" etc. mean both the commands input and the output arising from executing them, ie the responses.

FUJ00088036

4.0 Requirements

4.1 Areas of concern

There are two major areas of concern with the current support processes:

1. Second line support does not have the tools necessary to perform their function – i.e. tools to gather evidence from faults, which occur in the live system;
2. Third line and operational support organisations access to the live system is not fully audited and in some cases is unrestricted in the actions that can be carried out;

The consequences of these two issues are specified in the following sections.

4.1.1 Second line support

Second line support will have access to tools supplied by Tivoli; second line support staff will not be granted access to Counters via SSH.

4.1.2 Third line support

Third line support staff receives repeat instances of calls that should have been filtered out by second line. Handling repeat calls is not an affective use of third line support resource.

The current support practices were developed on a needs must basis; third line support diagnosticians had no alternative other than to adopt the approach taken given the needs to support the deployed Horizon solution.

The consequences of limited audit and system admin access afforded to third line support staff provide the opportunity to:

- Commit fraudulent acts;
- Maliciously or inadvertently affect the stability of the new Network banking and Debit Card online services;

In addition a complete audit would allow Pathway to defend the SSC against accusations of or fraud or misuse.

4.2 Support Categories

Support can be categorised into 4 groups:

1 first line (Help Desk) – receives calls from the customer regarding problems they are seeing at the counter. Where problems require it HSHD will document the call passing it onto another support unit;

2 Second line (SMC & HIT team) - are driven by two feeds – calls from other units and monitoring of the live system. It is their responsibility to match known problems against the diagnostic information available. Once matched they ensure the associated resolution action is carried out. New instances of faults are passed onto the relevant 3rd line support unit. The second line support function also includes those operational support units who are responsible for managing the infrastructure of the Horizon solution: hardware, network and OS support. Operational support access differs from other second line support units in that it

FUJ00088036

cannot operate with the restricted access associated with the SMC and HIT second line support teams. The access required by the operational support units is more in line with the access required by the third line support function (for data centres only, see 4.1.2).

3 Third line support (SSC and others) – handle those support calls that are not handled by either first or second line support. Third line support has access to application source code and therefore can identify new instances of faults providing an indication of where the fault occurred. Where a work around to the problem is identified this is documented within the KEL against a description of the problem. The KEL is used extensively by 1st and 2nd line support to resolve known problem.

4 Fourth line support – handle those calls that cannot be resolved by third line support. In addition fourth line support will provide fixes to identified faults.

4.3 Network banking an opportunity to fix

4.3.1 Second line support

To ensure second line support is able to carry out their function effectively the original solution defined access to the live system should be via a set of tools. These tools would have a number of basic security characteristics:

- All uses of a tool will be audited back to the individual who called the tools.
- Access to the tools will be role based with only authorised users being able to access a particular tool.

Tools were required to:

- The gathering of diagnostic information relating to specific problems
- Implementing fixes for issues identified during the data gathering

Due to various resourcing issues the second line support toolset has never been developed (see 0.7). It should be noted however, that the proposed SSH solution does not form part of this tool set but a mechanism for implementing auditability and access control.

The supportability requirements of the network banking service are documented as part of the non-function requirements, included in chapter 14 of the Infrastructure SDS. The requirements as documented include changes necessary to bring the current support practices in line with the definitions above, i.e. the provision of the support tools required by second line. The tools have been included within the network banking requirements because of the increased risk associated with not providing them.

The consequences of not developing the tools required by second line support is that third line support will continue to perform, as one of their tasks, the second line function. This is not a cost effective use of the highly skilled resources required to perform the third line support function.

Second line support tasks for NWB are defined in SY/SOD/006. SSH is providing the next level of support access i.e. where interactive diagnosis is required and defined Tivoli tasks will not provide adequately unencumbered access to remote systems.

FUJ00088036

4.3.2 Third line and operational support

All support access to the Horizon systems is from physically secure areas. Individuals involved in the support process undergo more frequent security vetting checks. Other than the above controls are vested in manual procedures, requiring managerial sign off controlling access to post office counters where update of data is required. Otherwise third line support has:

- Unrestricted and un-audited privileged access (system admin) to all systems including post office counter PC's;
- The ability to distribute diagnostic information outside of the secure environment; this information can include personal data (as defined by the data protection act), business sensitive data, and cryptographic key information.

The current support practices were developed on a needs must basis; third line support diagnosticians had no alternative other than to adopt the approach taken given the need to support the deployed Horizon solution.

There are however no automatic controls in place to audit and restrict user access. This exposes Fujitsu Services Pathway to the following potential risks:

- Opportunity for financial fraud;
- Operational risk – errors as a result of manual actions causing loss of service to outlets;
- Infringements of the data protection act;

4.4 Financial Fraud

Within the extant Horizon environment support staff are only able to exploit their privileged access, for fraudulent purposes, with the co-operation of counter staff. With the advent of Network Banking and Debit Card the dependency on counter staff can be eliminated. There now exists the opportunity to capture sensitive data and/or insert financial transactions by exploiting the maintenance and support accesses ability to replace code at the counter.

4.5 Operational risk

Unrestricted access to Horizon systems introduces the risk of destabilising the Horizon service, the ultimate consequence being loss of service at the counter. This is especially relevant with the advent of online application where data centre components are involved in real time communication with the counter.

The risks manifest themselves in the following ways:

- maliciously or inadvertent changes to Horizon systems causing reduced or even loss of the new on line services, including Network Banking and Debit Card;
- destabilisation of operational systems whilst they are hosting interactive diagnostic sessions:
    - by un-sized performance load;
    - by un-validated workload;

FUJ00088036

4.6 Controlled access to sensitive data

There are three categories of sensitive data within the Pathway solution:

- Personal data – subject to the rules of the data protection act regarding its storage, confidentiality, accuracy and use;
- Business sensitive data;
- Cryptographic keys / data;

None of the above sensitive data should be made available outside of the Pathway secure environment. Due to the potential sensitivity of cryptographic keys / data there is a further restriction that diagnostics that can contain this data:

- It can only be viewed by a defined group – initially the SSC third line support group and development;
- In a secure location – currently 6th floor in Bracknell and the secure room in FEL01;

4.6.1 Blue screen crash – screen image

If sensitive information is held in this file it will be extremely difficult to identify due to the small amount of data recorded.

4.6.2 Blue screen crash - Memory dumps

The Memory dump file is the only diagnostic information feed that can, practically, contain cryptographic material, and only then when the dumps originate from certain systems, including: post office counters, KMA server and agent servers. Memory dump files can also contain personal and business sensitive data.

4.6.3 Message store files

Extracts and complete Message store files will contain personal data; they will not include any unencrypted cryptographic keys. The personal data element means the access to the diagnostic information is subject the rules above regarding its distribution for support purposes.

4.6.4 Debit card Data files and error / trace log files

The Debit Card solution relies on a third party product: Solve/SE. This product makes no attempt to encrypt / obfuscate sensitive data contained within data files, error or trace logs. Third line and fourth line support groups will require access to these files and logs. Fourth line support will be provided by the third party supplier, our support contract with them will need to include clauses requiring them to review the output of log files at Pathway secure locations.

4.7 Security Requirements

The following security requirements are specified for support of Pathway systems:

- The design must define how the current method used by SSC to access counters is prohibited. The BI2 release included a Microsoft supplied security hot fix that closed off the security loophole being exploited by the SSC. A new route has been supplied,

FUJ00088036

this route is controllable in that is can be withdrawn once the solution documented in this SOD is implemented.

- In addition the design must show that Pathway systems can only be accessed for support activities by the authorised method;
- The existing secure VPN comms between the Data Centre and the Outlets is used as the link from the proposed Terminal Server hence the link encryption facilities provided by SSH are strictly unnecessary, SSH being used only for Authentication. Support access to other systems does not require link encryption as theses systems are either based at secure data centres, or in the case of remote FTMS servers, if the data transmitted warrants it the links used are already protected by line encryption.
- Authentication
    - The facilities provided by SSH encryption (between Client, on TS, and Server, on Counters), are to be used
    - Authentication when logging onto other, non-counter systems also needs to be considered, in particular when connecting to DCS platforms. These will be specifically identified by the SSH Client and will not have full command logging.
    - Authentication based on user names and passwords where the password is constantly changing based on a 'seed' common to both client and server is to be considered for the first implementation. Note the algorithm used will only be made available to the development unit and the Pathway security manager. Program code containing this algorithm will be secured by limited access.
- That the command audit facility of the Secure Shell (SSH) product from Cygwin (or similar) is used on the Terminal Server (see [NBSSH]). It will be necessary to enhance the current logging facilities as they were not designed to provide an audit of activities performed, rather a journal to remind the user of actions carried out.
- That the support users are only permitted read access to TS command audit logs.
- It is accepted that SSC will require full admin rights to Pathway systems, i.e. "they can do anything" it not being possible to place limits to there access for security reasons. Auditing of executed commands is considered an appropriate method by which control is administered, i.e. a complete record of all actions performed, by whom to what and when is maintained.
- That each SSC and operational support person has a separate account and that all logins to that account are audited (on the TS).
- That TS login can be correlated with the command audit log.
- That users are not able to switch off command auditing, access to the remote system will be denied if it is not possible to audit actions. No mechanism will be provided to relax this restriction, either functionally or procedurally. This will be mitigated by there being no single point of failure, e.g. more than one command logger per TS and an auto retry/reconnection on failure;
- TS support staff are to be available at all times SSC are available (and in practice should themselves be SSC personnel);

FUJ00088036

- Delivery of SSC written utilities to Pathway systems will be via Tivoli using a fast path configuration management route. Note the fast path route must include the following primary functions of the current configuration management process:
    - All files delivered plus the source code must be lodged in PVCS prior to be applied to the remote system.
    - An individual other than the developer of the task must carry out a minimum level of testing.
    - Tivoli will deliver the tool to the remote system having checked the CM generated digital signatures, ensure the delivered task is lodged in the PVCS configuration management system.
- The requirement for command logging is that all keystrokes input at the SSH Client are recorded as are all responses from commands executed on the SSH Server[4].
- Responses from a defined list of platforms will not be logged in full; only the first n bytes being logged. These platforms are those that hold sensitive data in clear. The list of 'excluded' platforms will be held under access controls such that normal Terminal Server users are not able to change the contents. Permissions for changing the list will be restricted and under authorisation of the Security Manager by OCP.
- The Terminal Server will be configured such that the TCP/IP connection between the Terminal Server and the Command Logger can only be monitored by the Terminal Server Administrator.

[4] It is recognised that this means that the logs will be difficult to interpret, however the over riding security requirement is that ALL actions an results are recorded no matter how difficult it is to interpret the results.

FUJ00088036

5.0 System Design

5.1 Principles of Secure support route

SSH will be used to provide the secure access to all remotely managed systems. Each system to be managed will include the SSH server within the platform build. A Pathway amended SSH client will be installed on a number of support terminal servers which will be located within the data centres. Access to the terminal servers will be via a terminal server client installed on the operational and third line support users workstation.

This design will be based on the OpenSSH implementation. In general wherever SSH is mentioned in this document it should be taken to mean OpenSSH.

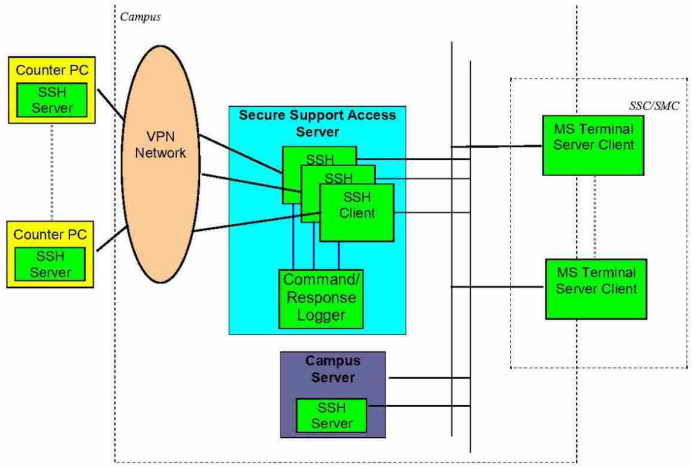

Figure 2: Overall SSH Architecture

5.1.1 SSH server

The OpenSSH server will need to be incorporated into the builds of all Pathway systems including, data centre servers, post office counters and remote FTMS gateways. Any platform that is an exception to this rule will be documented, registered and authorised by the Security manager, e.g. KMA Server.

The OpenSSH server will always be running on the counters. By default the cleardesk process will be amended to stop the SSH server and restart it[5]. The OpenSSH server will be modified to provide SSC user login using seeded password synchronised with the OpenSSH clients at the data centres.

[5] This is precautionary since although there is no need to shutdown and restart the OpenSSH Server this action will guard against memory leaks etc. Given the reliance being placed on this component such action may be advisable.

FUJ00088036

5.1.2 Counter Support user

A separate support user will be required on all counters.

- A standard username is created on all counter positions;
- The password is changed using an algorithm and seed values; the overall details of the algorithm and seed values remaining restricted;
- Full details of the algorithm will be available to the Security Manager who will be able to determine at all times the current password for all permissible users should the need arise, e.g. failure of password synchronisation;
- The password algorithm is coded into the SSH client running on the data centre terminal server and the SSH server running on counters and servers;
- The user will be a member of the administrators group on the counter or campus server as required to give the required access.

5.1.3 Secure Support Access Server.

The Secure Support Access Server (SSAS) will be based on Microsoft Terminal Server.

5.1.3.1 Additional Security domain

Third line and operational support units have, and require, system admin access to all systems they manage. In order to create a non-refutable audit of all actions carried out against systems they manage it is necessary to restrict their access to the system which is gathering the audit. The Horizon solution operates with a single security domain, administrators within this domain would have the ability to amend any audit generated if it was located within this security domain, and this is obviously unacceptable when considering the creation of a non-refutable audit.

A second security domain will be required, operational and third line support users will be operate as normal unprivileged users within this domain, the audit of actions carried out on the Horizon operational domain will be under the control of the administrators of the new security domain. The administrators of this domain will be available (for support) during the same period as the SSC in order to provide an adequately reliable service.

Changes will be required to the existing security NT domain hierarchy.

> *Question for Mark Ascot: Could this be as simple as moving the administration of the PWYDCS user domain to a separate group? ISD would no longer administer this domain however would have users within it who administer the Horizon resource domains.*

5.1.3.2 Platforms & Secure builds

A secure build for Microsoft Terminal Server will be required, plus corresponding changes to the user workstations to add the thin client software. Secure builds for these platforms will be fully documented and available only to Pathway Security TDA and the Pathway Security Manager.

Appropriate accounts will be required for the Terminal Server Administrator and Support Technicians. The Terminal Server Admin account must be such that it alone has full control on keys (OpenSSH host keys) and logging files; the support technician accounts would be

FUJ00088036

limited to read only access to these resources. If the proposed changes to the administration of the PWYDCS domain are made this activity can be achieved as follows:

- The terminal servers become member servers of the PWYDCS domain.
- Pathway operational service management users and SSC will have standard users rights within the PWYDCS domain.
- An alternative support unit will administer the PWYDCS domain.

A new terminal server platform build will be required. It is recommended a Windows 2000 server be used as opposed to NT 4.0 terminal server edition. The major advantage in using Windows 2000 server is reliability; the NT 4.0 terminal server edition is known to suffer from reliability issues.

5.1.4 SSAS Access

A terminal server client running on a support user workstation will be used to access the SSAS. The terminal server client will require the user to supply a username and password when they logon.

No shared usernames will be supplied all individuals will have separate support accounts within the PWYDCS domain. The desktop the user is presented with will depend on the users profile, which will in-turn depend on the role the user has. It is envisaged there will initially be three major roles; certain roles will have sub roles within them (for example the SMC has various levels depending on job title):

5.1.4.1 SMC role(s)

To be used by the second line SMC users. The profile for this role will be based on their role within the current Sysman domain. This role will include access to the Tivoli desktop, which will present users with all the Tivoli tasks they have access to.

In addition certain sub roles within the SMC role will have access to other tools which enable them to query the OMDB database. The ability to carry out local queries delay the upgrade of the links between the data centre and Stevenage. The SMC currently download large portions of the Tivoli events database to Stevenage in order to perform event analyse. This download consumes a large chunk of the available bandwidth and consequentially affects other applications/users that are trying to make use of the link. One particular application which cannot tolerate such a reduction in bandwidth is the SMDB; the SMDB will be used to alert the SMC and HSH to failures that affect the new style online services – Network Banking and Debit card. Performing the event analysis at the data centre removes the requirement to download the event information to Stevenage as the analysis will be carried out locally to the data. This has the added advantage to speeding up the event analysis process.

Exactly how the local query facility is provided will need further investigation.

The SMC desktop will not include access to the SSH client.

5.1.4.2 SSC role

The SSC desktop will include the following:

- SSH client

FUJ00088036

- Tivoli desktop
- Maestro GUI (read only)
- Others to be added following discussions with the SSC
- SSC Role to include SMC Role to provide access to 2nd line support tools

5.1.4.3 ISD role (Operational support)

The ISD (operational support) desktop will include the following:

- SSH client
- Maestro GUI
- Other management interfaces i.e. insite manager GUI's
- Others will be added following discussions with Core services

5.1.5 SSH client integration

The SSH product was selected for several reasons, primarily based on the availability of the source code thus enabling Pathway to:

- integrate the command/response logging audit capability;
- change the user password authorisation algorithm for Counter access.

The OpenSSH Client will integrated into the new build for the SSAS.

5.1.5.1 Key management

There will be no key material managed by the KMS.

Keys used by OpenSSH to establish connections (the "Host" keys) will be available to the SSH Server and the SSH Client as the result of their installation[6]. In the case of the SSH Client these will be held with access rights prohibiting the TS Client access.

5.1.5.2 Auditing user interactions

SSH.COM provides an SSH clients which supports command logging that could meet our audit requirement. Investigations into the use of SSH.COM's client shows logging can be easily switched on and off by the user, this is unacceptable for our solution.

The alternative is to modify the Open Source NT SSH Client to support command logging via sockets I/F to new Command Log server running on same host. This enables the socket client to reference the Server on the same host, i.e. the TCP/IP connection is built into the OpenSSH Client that it uses the same host for command log output. For resilience it is suggested that several Command Loggers are run concurrently. Failure of a Command Logger during a session will cause the OpenSSH Client to connect to an alternative. The Command Log server will be run under a higher privilege user to the OpenSSH Client and hence command logs will be secured.

[6] See [OSSH] section 5.4.4, "All SSH servers maintain a host key, which is persistent, generated by the system administrator when installing SSH, and identifies the host for authentication purposes".

FUJ00088036

SSH, client and server are available in source code form from http://www.openssh.org/ under the BSD licence. It is possible to build this product under Cygwin to run under Windows, this has been done and tested.

This opens the possibility of making changes to the source code to include mandatory logging of all commands and responses sent to and received by the client from the server.

The proposal is to change the OpenSource NT SSH Client such that it logs all commands and responses via a sockets I/F to new Command Log server running on same host. This enables the socket client to reference the command log server on the same host, i.e. it's built into the OpenSSH Client that it uses the same host for command log output, there being no configuration parameters or options to direct the output to any other destination. The Command Log server can run under a higher privilege user to the OpenSSH Client and hence command logs will be secured. By this design all security related and sensitive material on the support server can be made inaccessible from the standard, SSC / Operational support users. Only support personal with access to the support server administrator account will be able to access security related material; such users would by necessity have to have a higher level of security clearance and trust than 'standard' support users (see 5.1.3.1 above).

The initial communication between the SSC client and the command logger service will include the username of the person running the SSH client, the remote system they are connecting to and the date and time. The command logger service will service multiple client connections creating one log file for each connection. At the start of each log file the information sent as part of the initial communication will be logged. Once a session is complete the command logger service will close the file and move the file into an audit directory. The directory will be defined as an audit server audit point. The audit server will gather and stored the command logger files for 15 years. If the command logging service is unavailable then an SSH client will exit denying users access to remote systems. Note if there are several command logger then an alternative re-try strategy could be adopted to increase the likelihood of operating the service.

The SSH client will also be altered to get the username and password from a different source (when accessing Counter platforms), not requesting it from the user. The username will be available in the registry, the password being generated using the same password synchronisation algorithm used on the Counters.

5.1.5.3 SSH build related issues

By default the SSH server is delivered with other components, for example a secure FTP, SFTP etc. These functions must be excluded from the SSH client build installed on the terminal server. File transfer for the purposes of support will be provided by Tivoli. Note an alternative file transfer method for use when Tivoli is not working at the counters is to be considered, e.g. SCP (note this would require SCP to provide an audit log, currently this is not proposed).

Other GNU products may be required to facilitate access to the clients, the list will be the minimum required (by SSC and SMC), see Appendix B

5.2 OpenSSH

The Open SSH solution has 3 main components:

1 OpenSSH Server (to reside on all platforms)

FUJ00088036

2 OpenSSH Client (to reside on SSAS)

3 SSH Logger (to reside on SSAS – however should be developed such that it can run on an alternative platform, although for security reasons this will not be done, i.e. the connection between the Terminal Server and the logger will have to be secure).

The objective is to provide a secure environment via OpenSSH Client that will log all Support Staff keyboard interactions to file for Audit purposes. The interface will not support GUI interactions.

5.2.1 OpenSSH Server (on all platforms)

~~1.~~This is public domain software that is built under the 'cygwin' environment.

Formatted: Bullets and Numbering

It will be invoked as an NT service, started automatically and run continuously.

OpenSSH will be built for the 'cygwin' environment. Note: the 'cygwin' development environment must not be part of the installable product set.

Installation of 'cygwin' is normally interactive. For Pathway Counters (at least), this will need to be non-interactive – this is an additional development activity, see section 7.0.

Concurrent logins into the OpenSSH Server will be permitted.

Tool set to comprise only executables as in Appendix B No changes are to be made to the OpenSSH Server to add any Pathway functionality other than for password authentication.

5.2.2 OpenSSH Client (SSC Terminal Server)

This is public domain software that is built under the 'cygwin' environment. It will be invoked via users' desktops.

Ssh will be invoked via a command line that accepts a unique form of remote platform identifier, the properties of the addressing mechanism is to be determined, e.g. FAD Code for Counters, IP or hostname for servers. As described elsewhere in this document there are issues concerning the naming of remote hosts.

Once the remote host is connected, password processing will be as defined in section 5.1.5.2.

For each session, there is a pre-requisite that communication with the OpenSSH Logging Server exists. Any loss of the logger service will result in immediate loss or suspension (whichever is simpler) of all ongoing sessions.

As part of session establishment, the OpenSSH Client will report to the Command Logging Server the values defined in Table 1.

Command Log Field	Values	Notes
Timestamp		
Username of user account used to access the Terminal Server		
Username and group of OpenSSH Server account used		
Target hostname and IP address		Provide both are feasible

FUJ00088036

Command Log Field	Values	Notes
Unique session reference		
OpenSSH Client version in use		
OpenSSH Server version in use		
Reason code for opening session, see values column	PinICL, number to be included (checked against database?)	
	PowerHelp reference	
	OCP Reference (checked against database?)	

Table 1: Command Log Fields

The Logging Server must acknowledge receipt (by providing a session reference) before keystrokes can be sent to the remote host.

Upon completion of the session, a session-completion reason will be recorded to the Logging Server (to be stored in the session log – after which the log is closed and the session reference is released by the logger.).

All session output sent from the OpenSSH Server is to be logged by the OpenSSH Client to the Logger Service – to provide the auditor with a context.

The OpenSSH Clients will be configured with a set of servers name for which it will only record the start and end of the session together with the first n bytes[7]. The list of servers will include all those used for DCS (which will have sensitive data in clear at some time on the platform).

Installation of the OpenSSH Server will be non-interactive. No other tools will be installed on the local terminal server beyond the DLLs required for the operation of 'ssh'.

The Logging server will hold all logs in file store until they are audited by the Audit Server Maestro job.

The Development Team may require a Terminal Server installation on their platforms for the development and testing of the OpenSSH software.

To satisfy the no single point of failure requirement, multiple (4) SSAS's will be installed[8] deployed as to maximise resilience; if one is unavailable, users may use any of the other systems.

The development will conform to the SSC traceability requirements defined in TD/SDS/001 and in more detail in SY/SOD/001 – but only in areas where new code is written and it makes sense to increase traceability.

[7] The value of "n" is to be determined but should be small to limit the possibility of sensitive data being recorded in the log.

[8] There will be a Terminal Server platform for each SSAS.

FUJ00088036

Development must identify to ASD Security TDA any OpenSSH Client registry configuration parameters that require special 'lockdown' applied to the registry keys in order to secure their settings.

Re-boot of a platform running an OpenSSH Server will be recorded in the command log for all extant SSH connections to that platform.

SSH connections will be configured to use Keep-alives. FRIACO connections to counters will have no impact on SSH connections on establishment or during use of the connection; SSH will see the connection as standard TCP/IP[9].

All key stokes (including paste buffer contents on being actioned) will be time stamped with the time they are recorded by the OpenSSH Client, i.e. before being sent to the logger.

5.2.3 Command Logger (SSC Terminal Server)

This is a new piece of software that collects the output from the OpenSSH Client sessions and saves it into separate log files for each session. Two folders will be used one for 'live' sessions and one for 'completed' sessions. The audit server will collect files from the 'completed' folder.

The command logger will be started as an automatic NT service.

On start-up, any existing 'incomplete' session files in the 'live' folder will be terminated with a timestamp and reason for closure (i.e. 'logging restart') and moved into the 'completed' folder.

Upon request to start a new session, a new log-file will be created in the 'live' folder into which the details are logged. A reference is supplied to the OpenSSH Client to identify the session when further logging is necessary.

Upon completion of a session, the completion reason is stored. The session file is closed and then moved into the 'completed' folder.

Access to the log file area is restricted to the account under which the service runs and read-only access for support user accounts.

The audit server is responsible for the collection and long-term storage of the log files.

The command logger will not provide viewing/editing/management facilities for session log files.

Exceptions will be reported via NT Events – with Tivoli Event Collection as the mechanism for escalating problems. Any NT Events will not contain 'sensitive' information.

Although there will be four Terminal Server Platforms, the Command Logger will only accept logging session set-up requests from 'localhost', i.e. the same platform on which the OpenSSH Client is running[10].

The contents of session log files will be as defined in Table 1.

Installation of the product will be non-interactive.

---

[9] Note timeouts may need to be adjusted from their default values.

[10] If the Command Logger and OpenSSH client are to run on different platforms then the link between them will have to be protected, i.e. encrypted. Currently this is not proposed.

FUJ00088036

5.2.4 External (non-Estate Management) Activities

The following points need agreement with the staff/teams identified:

1. IPDU Security/PTI will need to develop SSC Terminal Server platform configurations to meet security roles and create desktops that meet the group definitions. Three groups of user will use the OpenSSH Client to access a platform

Group	Usage
SMC Group	May only use Tivoli desktop facilities to access platforms and there, they may run approved Tivoli packages only. Access to other Microsoft packages is required – including MS Access.
SSC Group	May use Tivoli Desktop and the new OpenSSH Client.
Operational Support	May use the new OpenSSH Client to Data Centre Platforms only (i.e. excluding Counters) and Maestro GUI.

Table 2: Terminal Server Groups

2. Usernames may need to be mapped to Roles. Roles mapped to Desktops. Desktops created with access to permitted toolsets (for Roles). Usernames will be unique.
3. (The software lists for the Desktops need to be fully defined – beyond the scope of the Estate Management Development.)
4. IPDU Security/PTI to create secure Logging Service user on SSC Terminal Server platform
5. IPDU Security/PTI to create SSC OpenSSH Server Service user on all Counter PCs
6. Maestro Schedules will be updated to trigger Audit Server to collect OpenSSH Logger files in encrypted format.
7. Audit Server is configured to collect and remove all files within the 'completed' folder.
8. Platform Build Designer (Kristine Neiras) will need to identify S/W and H/W components.
9. MSS will set up the Tivoli Event Collector – will need Application Event Lists from Support Guide Documentation when produced by Development.
10. PTI will perform the configuration of Terminal Server.
11. IPDU Infrastructure Release Team will provide a 'password juggling' DLL to generate the password for the required counter. Only SSC group users have access granted to use this DLL. Data Centre systems will use the native users NT accounts.
12. IPDU System Test will provide the first instance of a fully integrated environment (with Terminal Server and Secure users) under which OpenSSH Client will be invoked.
13. IPDU Secure Builds/AP Clients will need to lock down file store and apply registry level 'lockdown' to keys for OpenSSH Server, OpenSSH Client and Command Logger registry configuration parameters.

FUJ00088036

6.0 Systems Management

The SSAS will be managed by special support staff and will be available during all periods the SSC are themselves available.

SSH Client/Server password algorithm details will be under strict control of the Security Manager.

FUJ00088036

7.0 Application Development

The applications to be developed are:

- Enhancement to SSH Client to log commands;
- Command logging utility;
- Password synchronisation function;
- Non-interactive installation of the cygwin environment on Counters and Servers.

In addition the OpenSSH Client and Server configuration files will need to be developed.

The enhancements to the SSH Client (and OpenSSH Server if requires) will be undertaken such that it can be kept in line with the releases of OpenSSH.

Applications will be initially developed on non-Terminal Server configurations if possible although this is not a priority.

FUJ00088036

8.0 System Qualities

8.1 Availability

The system must provide 100% connectivity in a single point of failure environment, e.g. use of more than 1 terminal server at each campus.

8.2 Usability

There are no specific requirements for change in usability at BI3 for existing systems.

8.3 Performance

It is anticipated that there will be of the order of 100 users of this facility who in Terminal Server terms will be classified as "heavy users". The Terminal Server configuration to support this user population is:

- 2 Terminal Servers at each of 2 sites;
- each server has:
  - 2 processors
  - 2Gbytes memory
  - 36Gbyte hard disc.

Performance targets for the SSH connections are as follows:

- Static. 10 concurrent connections to an OpenSSH server when processing no traffic from the OpenSSH clients must have no more the 0.5% degradation on throughput of the server platform (i.e. counters or campus servers).
- Dynamic. As for static but no more than 1% degradation when 50% of the OpenSSH connections are processing 'typical' sessions.

FUJ00088036

8.4 Security

The subject of this SOD is security.

Support access to the Horizon solution is indirect, and recognised as not being formalised. The consequences of this approach result in:

- Possible financial fraudulent begin perpetrated by support staff – 70% of computer fraud is committed by internal staff;
- Exposure of support staff to accusations of fraud access – we cannot prove such access is not possible;
- Operational issues ultimately resulting in loss on service at one or more outlets.

Contractually Fujitsu Services Pathway is required to adhere by the agreements as documented in the codified agreement, summarised by compliance to the ISO 17799 security specification and PACE[11] standards. Fujitsu Services Pathways adherence to these standards is demonstrated by our implementation of the policies set out in the SFS and ACP. The SFS/ACP requires all access to Horizon systems is identifiable back to the individual, with access being granted on the basis of the minimum required.

8.4.1 SSH Authentication

SSH performs two levels of authentication:

- Server authentication, where the client verifies the identify of the client and server
- User authentication, where then server verifies the identity of the user requesting access.

These authentication processes are considered adequate.

All SSH traffic to counters and campus servers will be encrypted, in the case of counters it will be doubly encrypted.

Platforms, which have sensitive data in clear, will not have the results of commands directed to them audited.

Only authorised support staff will undertake support of Terminal Servers.

Normal support users will not have access to modify the behaviour of the Terminal Servers or SSH clients and servers.

8.5 Potential for Change

None identified

8.6 Migration

The recommended migration strategy is:

1. Before the main S30 release the terminal servers and client software are installed;
2. SSH is added to a few selected platforms and tested/evaluated;

[11] PACE – information from the Pathway system will be used as prosecution evidence in fraud cases. The integrity of the data made available for this purpose must be assured

FUJ00088036

3. Main S30 release the other platforms are converted to SSH, rclient is left installed but disabled;
4. At the next release (S40?) rclient is removed from the rigs.

FUJ00088036

9.0 Solution Implementation Strategy

The solutions strategy will be to

- modify SSH client and server;
- implement Command Logging server
- implement password synchronisation algorithm
- implement TS environment plus TS thin clients
- implement SSH configurations for Counters and Campus environments
- implement audit integration
- implement security processes and procedures
- implement Tivoli download scripts for SSH server installations

Changes to the OpenSSH client and server code will be undertaken such that the impact of bug fixes on these open source components is minimised.

FUJ00088036

10.0 Testing Strategy

Due to the high reliance placed on this development to support the Pathway system testing should be undertaken in an environment close to live as possible. This will require the following platforms and systems together with associated software products, e.g. OpenSSH Client and Servers, Command Logging Service, Tivoli, Maestro etc:

- Terminal Server and network-connected client support work stations
- FRIACO network (including ISDN call out)
- Firewalls configured for worst case i.e. NWB and DCP DMZ
- Multi-counter outlet configuration
- Single-counter outlet configuration
- Representative campus servers
- Audit server

Note that other than for performance testing the test Terminal Servers do not have to be to "live" configurations, as they will not be correspondingly loaded.

Testing for viability during high Tivoli traffic periods, e.g. UAR must be considered.

FUJ00088036

11.0 Cost, Risks and Timescales

Costs and timescales are being handled as part of the planning process.

11.1 Risks

The following risks have been identified:

- OpenSSH V3.2 has been the subject of a security advisory. This has been removed in V3.4.
- Security alerts may be commonplace for the base OpenBSD version of the public domain S/W. Source for the portable OpenSSH is subsequently changed AFTER the OpenBSD changes have been issued. Security will need to monitor and assess risks and to request further redelivery of the revised code from development when necessary. Note assessing the risk of security alerts is required of all software products, proprietary or open source. However notification and time to correction of open source products can often be significantly better than proprietary products, e.g. NT.
- SSC/SMC buy in to the limitations of functionality.
- SSC agreement to additional operational level to administer security aspects of Terminal Servers.

11.2 Timescales

BI3 S30

FUJ00088036

APPENDIX A SECURE SHELL

The Secure Shell Protocol provides support for secure remote login, secure file transfer, and secure TCP/IP and X11 forwardings. It can automatically encrypt, authenticate, and compress transmitted data. The objective of SSH include that it:

- provides strong security against cryptanalysis and protocol attacks,
- can work reasonably well without a global key management or certificate infrastructure,
- can utilize existing certificate infrastructures (e.g., DNSSEC, SPKI, X.509) when available,
- can be made easy to deploy and take into use,
- requires minimum or no manual interaction from users,
- is reasonably clean and simple to implement.

The resulting protocol will operate over TCP/IP or other reliable but insecure transport. It is intended to be implemented at the application level.

The SSH Protocol comprises:

- SSH Transport Layer Protocol
- SSH Authentication Protocol
- SSH Connection Protocol
- SSH Protocol Architecture
- Generic Message Exchange Authentication For SSH
- SSH File Transfer Protocol
- GSSAPI Authentication and Key Exchange for the Secure Shell Protocol
- SECSH Public Key File Format
- Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol
- Storing SSH Host Keys in DNS
- SSH Agent Forwarding

A.1 Threats SSH Can Counter

- Eavesdropping
- Name Service and IP Spoofing
- Connection Hijacking
- Man-in- the middle attacks

FUJ00088036

- Insertion attack

A.2 Threats SSH Doesn't Prevent

- Password cracking
- IP and TCP attacks
- Traffic analysis
- Covert channels
- Carelessness

FUJ00088036

APPENDIX B COMMANDS FOR SSC USE

The commands in this appendix will be additional to their Tivoli equivalents in order that any changes to the Tivoli set do not impact the secure access capability.

This appendix details commands required by SSC in bash environment. Availability of commands marked as "**?**" is to be reviewed.

B.1 File content Commands

Command	Description	
cat	Concatenate files and print on the standard output	
cmp	Compare two files byte by byte	
cut	Remove sections from each line of files	
dd	Convert and copy a file	
diff	Compare files line by line	
egrep	Print lines matching a pattern	
fold	Wrap each input line to fit in specified width	
gzip/gunzip	Expand / compress file	
head	Output the first part of files	
less	File viewing	
md5sum	Compute and check MD5 message digest. (Checksum files to compare against known good file)	
nawk	Manipulate files (automate multiple search replace in files)	
nl	Number lines (Determine postition in error by line number)	
od	Octal / hex dump (Examine file at binary level)	
paste	Merge lines of files	
sed	Stream editor (Minor file changes / Edit variables in scripting)	
sort	Sort lines of text files	
tail	Output the last part of files (Check end of large error log without going through whole file)	
tar	Saves many files together into a single tape or disk archive (Process a set of files for import/export in conjunction with gzip)	
tee	Read from standard input and write to standard output and files (Produce action logs while doing work)	
touch	Change file timestamps	
wc	Print the number of bytes, words, and lines in files	

FUJ00088036

B.2 Filesystem Commands

Command	Description	
chgrp	Change group ownership (permissions manipulation)	?
chmod	Change file access permissions (permissions manipulation)	?
chown	Change file owner and group (permissions manipulation)	?
cp	Copy files and directories	
df	Report filesystem disk space usage	
du	Estimate file space usage	
find	Search for files in a directory hierarchy	
ln	Make links between files	
ls	List directory contents	
mkdir	Make directories	
mount	Manipulate mount points	?
mv	Move (rename) files	
pwd	Print name of current/working directory	
rm	Remove files or directories	
rmdir	Remove empty directories	
umount	Manipulate mount points	?

B.3 Process control Commands

Command	Description	
kill	Kill process	
nice	Run a program with modified scheduling priority	
ps	Show process uids, ppids	
sleep	Delay for a specified amount of time	

B.4 Scripting Commands

Command	Description	
basename	Strip directory and suffix from filenames	
date	Print or set the system date and time	
dirname	Strip non-directory suffix from file name	

FUJ00088036

Command	Description	
echo	Display a line of text	
expr	Evaluate expressions	
false	Do nothing, unsuccessfully (used in script tests)	
printf	Format and print data	
true	Do nothing, successfully (Used in script tests)	
test	Check file types and compare values	

B.5 Other Commands

Command	Description	
chroot	Run command or interactive shell with special root directory (run tools in protected subset of filestore)	
cygpath	Convert windows filenames to posix	
hostname	Set or print the name of the current host system	
login	Change user name	?
regtool	Manipulate windows registry	
tset	Terminal initialization (reset terminal / clear screen after errors)	
tput	Manipulate terminfo (setup terminal type correctly)	

B.6 Tools location and Sizes

Tivoli column indicates old Tivoli tools already present in c:\tivlcf\lcf\bin\w32-ix86\tools and require cygwinb19.dll to run. Compressed (zip) is 962,451 bytes

Command	Size (Bytes)
Basename	19456
Cat	17408
Chgrp	30720
Chmod	30208
Chown	32256
Chroot	19968
Cmp	18432
Cp	77312
Cut	18944
cygpath	11264
date	49152
dd	41472
df	39936
diff	87040

FUJ00088036

dirname	18944
du	38912
echo	19968
egrep	85504
expr	50688
_false	13312
find	78848
fold	16896
gzip	50176
head	18944
hostname	19456
kill	4608
less	95744
ln	60416
login	14336
ls	68608
md5sum	32256
mkdir	30720
mount	10240
mv	83968
nawk	169984
nice	20480
nl	45568
od	31232
paste	15872
printf	24064
ps	10752
pwd	18944
regtool	12288
Reset (->tset)	30720
rm	65024
rmdir	25088
sed	46592
sleep	18944
sort	40448
tail	33280
tar	146944
tee	20480
test	32256
touch	39424
tput	10240
_true	13312
umount	7680
wc	23552
Total	**2209280**

FUJ00088036

APPENDIX C OPENSSH CONFIGURATION

C.1 Openssh Server Configuration

See sshServer config for description of each parameter.

Option	Parameters	Notes
AFSTokenPassing	Default	
AllowGroups	TBD	Admin users
AllowTcpForwarding	No	
AllowUsers	TBD	
AuthorizedKeysFile	default	
Banner		Legal warning msg TBD: "*This session is being recorded and may be used as evidence in legal proceedings*"
ChallengeResponseAuthentication	Default	
Ciphers	None	
ClientAliveInterval	Default	
ClientAliveCountMax	Default	
Compression	Default	
DenyGroups	TBD	
DenyUsers	TBD	
GatewayPorts	Default	
HostbasedAuthentication	Yes	
HostKey	TBD	
IgnoreRhosts	Default	
IgnoreUserKnownHosts	TBD	
KeepAlive	Default	
KerberosAuthentication	Default	
KerberosOrLocalPasswd	Default	
KerberosTgtPassing	Default	
KerberosTicketCleanup	Default	
KeyRegenerationInterval	Default	
ListenAddress	TBD	
LoginGraceTime	60	
LogLevel	Default	

FUJ00088036

Option	Parameters	Notes
MACs	Default	
MaxStartups	Default	
PasswordAuthentication	Default	
PermitEmptyPasswords	Default	
PermitRootLogin	No	
PidFile	Default	
Port	TBD	
PrintLastLog	Default	
PrintMotd	No	
Protocol	Default	
PubkeyAuthentication	No	
RhostsAuthentication	Default	
RhostsRSAAuthentication	Default	
RSAAuthentication	No	
ServerKeyBits	Default	
StrictModes	Default	
Subsystem	Default	
SyslogFacility	Default	
UseLogin	Default	
UsePrivilegeSeparation	Default	
VerifyReverseMapping	Default	
X11DisplayOffset	0	
X11Forwarding	Default	
X11UseLocalhost	Default	
XAuthLocation	Default	

C.2 Openssh Client Configuration

See sshclient config for description of each parameter.

Option	Parameters	Notes
AFSTokenPassing	Default	
BatchMode	Default	
BindAddress	Default	

FUJ00088036

Option	Parameters	Notes
ChallengeResponseAuthentication	Default	
CheckHostIP	No	
Cipher	""	
Ciphers	TBD	
ClearAllForwardings	Yes	
Compression	Default	
CompressionLevel	Default	
ConnectionAttempts	Default	
DynamicForward	No	
EscapeChar	None	
ForwardAgent	Default	
ForwardX11	Default	
GatewayPorts	Default	
GlobalKnownHostsFile		
Host	TBD	
HostbasedAuthentication	Default	
HostKeyAlgorithms	Default	
HostKeyAlias	TBD	
HostName	TBD	
IdentityFile	TBD	
KeepAlive	Default	
KerberosAuthentication	No	
KerberosTgtPassing	No	
LocalForward	No	
LogLevel	Default	
MACs	Default	
NoHostAuthenticationForLocalhost	TBD	
NumberOfPasswordPrompts	Default	
PasswordAuthentication	Default	
Port	Default	
PreferredAuthentications	hostbased	
Protocol	Default	
ProxyCommand	TBD	
PubkeyAuthentication	No	
RemoteForward	No	
RhostsAuthentication	Default	
RhostsRSAAuthentication	Default	
RSAAuthentication	No	
SmartcardDevice	Default	
StrictHostKeyChecking	Yes	
UsePrivilegedPort	Default	
User	Support Admin	Actual name TBD
UserKnownHostsFile	Default	
XAuthLocation	Default	