STANFORD
UNIVERSITY

INFORMATION TECHNOLOGY SERVICES

PGP Proof of Concept Completion Checklist

Updated as of November 7, 2008

Proof of Concept Start Date: September 23, 2008

Proof of Concept Completion Date: October 31, 2008

Proof of Concept Objectives			
	Yes	**No**	**Comments**
Proof of Concept objectives defined and completed	✓	☐	Defined in initial SGG Project Charter under Expected Deliverables and Timeline
Proof of Concept Budget approved	✓	☐	October 23, 2008 - $55,000
Proof of Concept completed no later than October 31, 2008?	✓	☐	Email confirmation to participating testers on November 3, 2008
Proof of Concept completed within Budget	☐	☐	Expenses incomplete Estimated to be within approved budget
Go/No Go Decision made?	✓	☐	Recommendation is to proceed with PGP for Stanford's Whole Disk Encryption Solution for Mac and Windows computers/platforms
Proof of Concept Initiation			
	Yes	**No**	**Comments**
Key Participants identified and available to participate	✓	☐	WST, Tier 2 Help Desk, CRC, PMO
Acquire Initial Set of PGP licenses – Mac/Win	✓	☐	Purchase via PCard for initial licenses – 10 Win, 10 Mac, 20 Universal Server
Project Manager Assigned	✓	☐	Steve Loving
Initial Testers volunteered and representative of the on-going support organizations	✓	☐	Identified 19 testers across WST, Storage, Integration, Tier 2 Help Desk, Desktop Systems Group, and CRC
Evaluation and Testing Objectives			
	Yes	**No**	**Comments**
Initial Test Whole Disk Encryption <u>Stand Alone client</u>			
Successful download of the WDE client	☐	✓	Significant struggle using the web download ability with all 20 licenses identified for Bruce Vincent. Brute force required. Impacted ~ 1/3 of testers who did not actively participate. NON ISSUE with Universal Server

	Yes	No	Comments
Windows (XP, Vista)			
Intuitive login to WDE Workstation	☐	✓	Requests PGP passphrase which is not intuitive. Can address by customizing initial PGP screen and providing directions. Sign in process will require two steps – PGP and the traditional login.
Initiate and successfully complete WDE Encryption process	✓	☐	Time required for Encryption varies by platform (OS) and size of hard drive. Suggest this be started towards end of the day and run throughout the evening. Recommend run on AC power, not battery.
Acceptable performance of workstation with WDE	✓	☐	Impact noticed when downloading large video files (~18Gb)
Existing files/folders that were encrypted prior to PGP are accessible to the user	✓	☐	The WDE encryption simply adds an additional layer of encryption (done at disk level, not file level)
Macintosh (MacIntel, 10.4+)			
Intuitive login to WDE Workstation	☐	✓	Requests PGP passphrase which is not intuitive. Not yet able to customize initial PGP screen and provide directions. Sign in process will require two steps – PGP and the traditional login.
Initiate and successfully complete WDE Encryption process	✓	☐	Time required for Encryption varies by platform (OS) and size of hard drive. Suggest this be started towards end of the day and run throughout the evening Must run on AC. Encryption stops on battery and requires Decryption and restarting of Encryption process.
Acceptable performance of workstation with WDE	✓	☐	Impact noticed when downloading large video files (~18Gb)
Existing files/folders that were encrypted prior to PGP are accessible to the user	✓	☐	The WDE encryption simply adds an additional layer of encryption (done at disk level, not file level)
Installation and Configuration of Universal Server			
Identify Server for Proof of Concept	✓	☐	
Install and configure Universal Server appliance	✓	☐	
Intuitive Interface for Logging and Reporting	✓	☐	
Key Logging/Reporting Components available	☐	✓	Stanford specific audit reports may be required
Intuitive Interface for Whole Disk Retrieval Token	✓	☐	
Key Retrieval Components available	✓	☐	
Ease of Integration with Active Directory	☐	✓	Will need to be developed

Ability to change key settings to meet Stanford's needs	✓	☐	Ability to not allow user to decrypt without "Help Desk" assistance
Ability for distributed IT Support groups to manage within Universal Server	☐	✓	Access to one system within Universal Server allows access to ALL systems and recovery tokens. Retain Universal Server access within IT Services
Initial Test Whole Disk Encryption with Universal Server			
	Yes	**No**	**Comments**
Windows (XP, Vista)			
Installation of WDE client via Universal Server process	✓	☐	
Intuitive login to WDE Workstation	☐	✓	Requests PGP passphrase which is not intuitive. Can address by customizing initial PGP screen and providing directions. Sign in process will require two steps – PGP and the traditional login (installer modification required to enable secondary login requirement)
Initiate and successfully complete WDE Encryption process	✓	☐	Time required for Encryption varies by platform (OS) and amount of disk. Suggest this be started towards end of the day and run throughout the evening. Recommend run on AC power, not battery, as battery power will pause encryption.
Acceptable performance of workstation with WDE	✓	☐	Impact noticed when downloading large video files (~18Gb)
Initial evaluation Whole Disk Encryption Workstation Backup/Recovery/Backup Size with both Mozy and Iron Mountain	✓	☐	Mozy and Iron Mountain appear to do an initial full backup, followed by incremental backups
Existing files/folders that were encrypted prior to PGP are accessible to the user	✓	☐	The WDE encryption simply adds an additional layer of encryption (done at disk level, not file level)
Macintosh (MacIntel, 10.4+)			
Installation of WDE client via Universal Server process	✓	☐	
Intuitive login to WDE Workstation	☐	✓	Requests PGP passphrase which is not intuitive. Not yet able to customize initial PGP screen; provide directions. Sign in process will require two steps – PGP and the traditional login.
Initiate and successfully complete WDE Encryption process	✓	☐	Time required for Encryption varies by platform (OS) and size of hard drive. Suggest this be started towards end of the day and run throughout the evening Must run on AC power. Encryption continues on battery power, but will require Decryption and restarting of Encryption process if machine loses power during the Encryption process.

Acceptable performance of workstation with WDE	✓	☐	Impact noticed when downloading large video files (~18Gb)
Initial evaluation Whole Disk Encryption Workstation Backup/Recovery/Backup Size with both Mozy and Iron Mountain	☐	☐	NOT COMPLETED Mozy appears to do an initial full backup, followed by incremental backups
Existing files/folders that were encrypted prior to PGP are accessible to the user	✓	☐	The WDE encryption simply adds an additional layer of encryption (done at disk level, not file level)
Vendor Relationship			
	Yes	**No**	**Comments**
Is the Vendor Relationship collaborative?	✓	☐	Cooperative and collaborative to date
Are skilled consultants available and able to participate in the success of this project	✓	☐	Via PGP Resellers
Security and Architecture Review			
	Yes	**No**	**Comments**
Initial review of PGP Architecture/Security with appropriate Stanford and PGP representatives	✓	☐	Held October 30, 2008 at PGP
Initial review of Architecture aligns with Stanford's current services and infrastructure	✓	☐	Design includes Master/Slave Servers. Decision will need to be made related to the potential risks of the users and the level of PGP Support Agreement we require.
Initial review of Security risks meet Stanford's acceptance level	✓	☐	

General Observations as a Result of the PGP Proof of Concept

The general observations of the PGP Proof of Concept is that this is a viable solution for Stanford University's business need to provide encryption solutions to Windows, Macintosh and ultimately Linux desktops and laptops that may hold Prohibited, Restricted and/or Confidential data.

The recommended solution is to use the PGP Whole Disk Encryption (WDE) solution leveraging the PGP Universal Server.

There are decisions to make regarding:

- Confirming Best Practices associated with this Encryption Offering to increase the confidence of the state of the data in the event a desktop/laptop and in the future PDA is lost/stolen
- Licensing the software by User or by Device
- Protecting Stanford owned equipment only or including any desktop/laptop used by anyone with SUNet id

This PGP solution is the preferred solution at Yale, parts of Harvard, Baylor, and University of Colorado. The determining factor is predominantly a single solution for both Windows and Mac desktops/laptops.

Actions to address during PGP Whole Disk Encryption Deployment Project

Action Item
Determine implications to PGP WDE user in the event the Master Universal Server is unavailable. Identify alternatives as needed. Determine if Business Continuity requires a second Master available on campus or in Livermore
Scope Integration needs between Stanford's Active Directory and the Universal Server
Determine who the target audience is for the PGP WDE service. - any one who wants to use the service - require if Prohibited, Restricted and/or Confidential data on desktop/laptop - All Faculty? All Staff? Students? - Stanford equipment only or any device associated with an active Stanford SUNet ID member
Clearly identify and document the expectations of the user of PGP's Whole Disk Encryption service
Confirm if this service will be provided with or without a fee to the user or department organization
Create Project Plan, Milestones, Cost Estimate/Resources and Charter