HP ProtectTools Client Security Manageability for Enterprise Customers with Managed IT

All information in this document is for use by HP customers and channel partners.

Table of Contents

Introduction and Summary

Enterprise systems developers struggle to provide a unified interface for their security infrastructures that includes access control, drive encryption, single sign-on, policy management, administration and auditing. Organizations that are focused on improving their levels of security are looking to address the manageability of these critical security issues, including:

- Secure and accessible credential information for each user and secure access to all services, regardless of network connectivity or server load
- Management of increasingly disparate applications, each with a proprietary authentication mechanism, directory and usage limits
- Ability to address differing enterprise security requirements across multiple organizations, whether federally mandated or management-directed
- Enterprise-level vs. client-level deployment through an IT administrator for HP platforms
- And more…

Security manageability for HP ProtectTools can be delivered by HP and its strong relationship with key security vendors. HP, working with these key security vendors, jointly developed the HP ProtectTools security software suite modules that provide protection to the client. And, with direct engagement from these vendors centralized manageability of these security modules can be functional.

The purpose of the **HP ProtectTools Client Security Manageability for the Enterprise Customer with Managed IT** white paper is to provide you with the information on HP's key security vendors, discuss the appropriate vendor to meet each of your needs, provide you with HP recommendations that will make manageability of security a reality, and give you the details so you know where to begin.

Beyond this white paper, additional materials are available for review. These include:

- **Vendor Data Sheets:** Vendor-specific collateral is available as noted in the **For More Information** section at the end of this white paper. Each vendor has been validated by HP and can provide you with security manageability.
- **Vendor Whitepapers:** These whitepapers are available as noted in the **For More Information** section at the end of this white paper. The vendor has provided information on their deliverables and engagement process so your expectations can be properly met.

Figure 1. HP ProtectTools client security manageability delivered by key security vendors

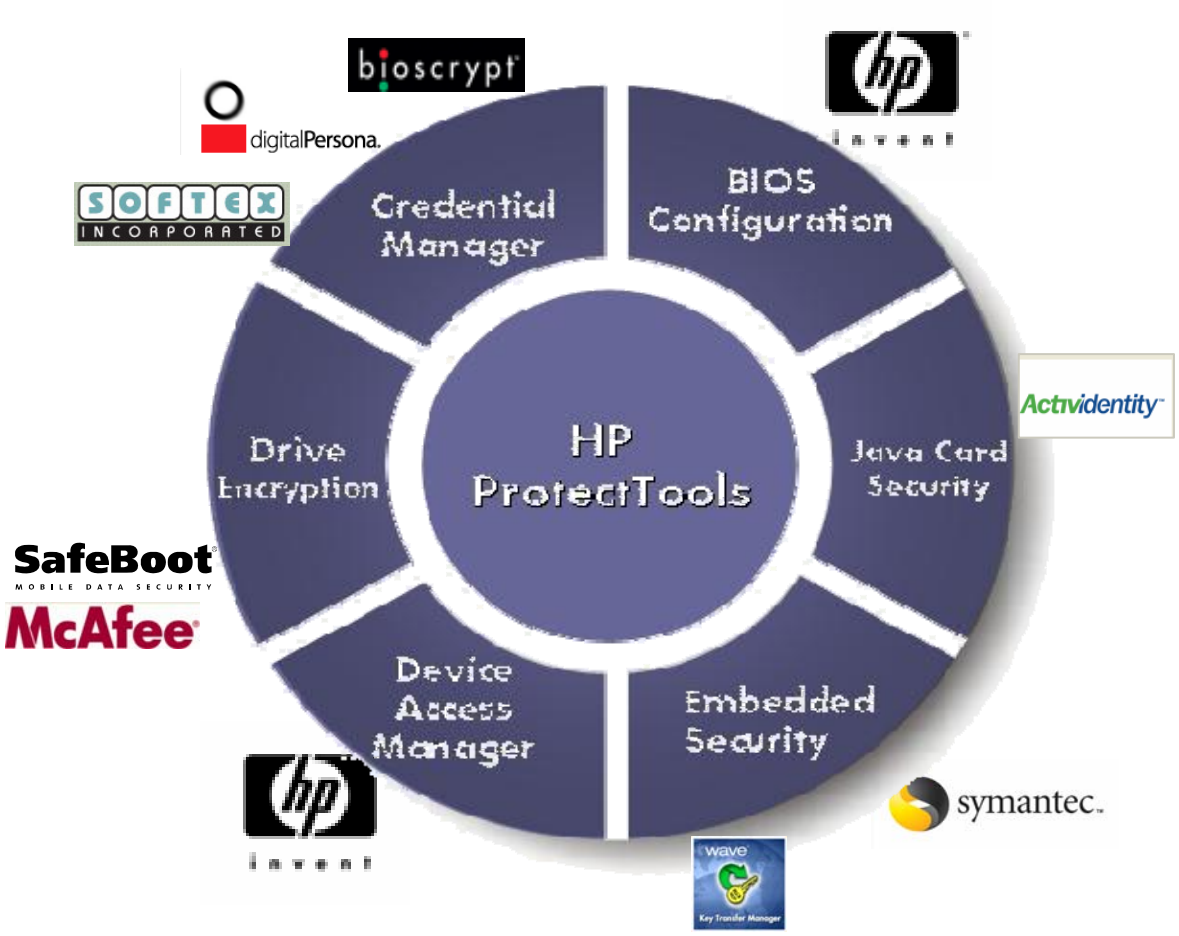

Figure 2. Matrix of vendor capabilities

Security Manageability Vendor Matrix												
Customer Needs	Customer Use Cases	HP C&I	HP Software	Symantec	MS SMS	Wave	McAfee	Activ Identity	Bioscrypt	Digital Persona	Pointsec Utimaco	Softex
Deploying HP ProtectTools	**Scenario 1**											
I want to deploy HP ProtectTools	Case A		●	●	●							
I need to update security settings and enforce policies	Case B	●	●	●	●	●	●	●	●			
Strong Authentication Policies	**Scenario 2**											
I need to enforce strong authentication policies across the network with biometrics	Case A								●	●		
I need to enforce strong authentication policies across the network with smart cards	Case B							●				
I need to enforce strong authentication policies across the network using credential roaming	Case C								●			
Strong Single Sign On Authentication Policies	**Scenario 3**											
I need strong authentication policies with enterprise single sign-on and remote biometric authentication	Case A							●	●			
I need strong authentication policies with enterprise single sign and remote smart card or token authentication in multiple domain environments	Case B							●	●			
Full Volume Encryption	**Scenario 4**											
I need to implement full volume encryption	Case A						●					
TPM	**Scenario 5**											
I need to initialize and enable the TPM	Case A		●	●	●	●						●
I need to utilize the TPM to enhance Drive Encryption	Case B		●				●				●	
I need to utilize the TPM to enhance Drive Encryption with biometric authentication	Case C											
I need to utilize the TPM to enhance Drive Encryption with smart card or token authentication	Case D						●	●				
I need to utilize the TPM for protected VPN access	Case E	●				●						●
I need to utilize the TPM with key management	Case F	●				●						●
Device Control	**Scenario 6**											
I need to limit users to read only	Case A	●										

Use Cases and Recommendations

Overview of HP ProtectTools Deployment

HP ProtectTools is the client security software solution **for HP environments**. Manageability of HP ProtectTools modules is accomplished through the use of HP or its key security vendors who jointly developed each client module with HP. Since the client modules function together smoothly, the manageability software provided by each security partner should function together smoothly as well. For **multi-vendor environments**, security can be provided by combining HP ProtectTools in conjunction with vendor solutions.

This section will discuss the options available in order to deploy HP ProtectTools and any combination of plug-in modules. This section is a prerequisite to the following sections in case of an HP-only environment where the solution requires any HP ProtectTools module.

Scenario 1 - Security implementation

Case A: Deployment

Deployment of HP ProtectTools on all HP business clients can be accomplished by various means. The client software on HP notebook, desktop and workstation platforms are either preinstalled, available on the web in SoftPaqs or, for select desktop and workstation platforms, available as an After Market Option (AMO) on HP.com

For manageability of these clients, you will need to engage with your HP representative and the following partners, depending on the size of your infrastructure and your needs.

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• HP Client Automation • HP Client Manager 6.2 • Microsoft ® System Management Server (SMS) with HP System Software Manager (SSM)	• HP platforms are manageable as advised for the exclusive HP Platform • There is no universal manageability for HP ProtectTools on non-HP platforms. Individual modules can be deployed through key security vendors	• Use HP Client Automation, HP Client Manager (Symantec based), or Microsoft SMS with HP System Software Manager (SSM) for HP ProtectTools SoftPaq deployment. • Information available (such as white papers, additional product information, etc.) at www.hp.com/go/easydeploy

Case B: Implementing, deploying and updating security policies and settings

Monitoring, deploying and enforcing security policies and settings is a function of the modules that have been deployed. This includes migration capabilities of moving profile and key data from one PC to another and ensures backup/restore functionality and compliance with implemented policies.

HP Technical Consultants should be included to take a proactive role in facilitating the process, ensuring that your expectations are met or exceeded.

Many different technologies function together inside HP ProtectTools and you can choose to implement all or a sub-set of those technologies to meet your requirements. HP relies on key security vendors as well as internal organizations to develop HP ProtectTools modules, and management of the components can vary. In all cases, the business model is that HP works alone or with vendors to develop and provide software designed for a single user on the appropriate HP platforms with the enterprise version of the software being available through HP or the vendor. These vendor solutions can typically result in lower cost for HP platforms due to the fact that HP platforms come preconfigured with the single user pre-licensed.

Depending on the module, remote management capability will vary and sometimes multiple solutions will be necessary to deploy. For the enterprise customer with Managed IT, the HP ProtectTools capabilities that will need to be controlled are:

- BIOS settings
- Drive Encryption (Full Volume Encryption)
- Smart Card
- Biometrics
- Single Sign On
- Device Access Manager
- Trusted Platform Module (TPM)

	Security manageability partners		
	Hardware environment		
Capabilities	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
BIOS Settings	•HP Client Automation •HP Client Mgr 6.2 •Microsoft SMS w/HP SSM	There is no universal standard available for managing BIOS across vendors. Use solutions as defined in this document for HP platforms, and BIOS vendor tools for non-HP platforms.	HP Client Automation and HP Client Manager (Symantec based) are very good tools for BIOS setting deployment. They are WMI capable and work with WMI enabled BIOS developed for the 2006 platforms and later. For older systems, HP provides HP Client Management Interface, a WMI software provider. Microsoft SMS with HP SSM can set the BIOS settings. Additional information is available on white papers, product data, etc. at www.hp.com/go/easydeploy.

	Security manageability partners		
	Hardware environment		
Capabilities	Exclusive HP	Multi-Vendor	HP Recommendation
Drive Encryption (Full Volume Encryption)	McAfee Endpoint Encryption	McAfee Endpoint Encryption	See Scenario 4
Smart Card	ActivIdentity	ActivIdentity	See Scenarios 2, 3, 5
Biometrics	Multiple Options	Multiple Options	See Scenarios 2, 3, 4, 5
Single Sign On	Multiple Options	Multiple Options	See Scenarios 2, 3
Device Access Manager	HP Enterprise Device Manager	HP Enterprise Device Manager	See Scenario 6
TPM	Multiple Options	Multiple Options	See Scenario 5

Scenario 2 - Strong authentication policies

Authentication support in the Windows environment is provided by HP ProtectTools Security Manager using Credential Manager for HP ProtectTools. Credential Manager supports multiple authentication technologies centrally, and has the capability to combine the different authentication devices to provide multifactor authentication policies.

The ability to manage multiple authentication technologies centrally from within a single application means you can deploy different authentication technologies across your enterprise depending on suitability to task. This also means you can create complex authentication processes by combining two or more authentication devices for stronger security.

	Security manageability partners		
	Hardware environment		
Customer	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
Managed IT	• Bioscrypt • Wave	• Bioscrypt • Wave	• Bioscrypt was the primary collaborator in developing Credential Manager for HP ProtectTools. Verisoft Single Sign On by Bioscrypt is enterprise software and does not require the additional purchase of the client version for HP platforms that have HP ProtectTools installed. • Alternatively, if TPM key management is required in addition to strong authentication, then Wave's EMBASSY Trust Suite is an excellent option.

Case A: Network biometric authentication

Biometric fingerprint authentication provides convenient, easy to use authentication that is more secure than simply utilizing weak passwords.

	Security manageability partners		
	Hardware environment		
Customer	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
Managed IT	• Bioscrypt • Digital Persona	• Bioscrypt • Digital Persona	• Bioscrypt's Verisoft Single Sign On (Server) was built for the multi-factor environment with any combination of biometrics, smart cards, tokens, TPMs, etc. • DigitalPersona Pro (Server) is built specifically for biometrics and works with Microsoft's standard password and smart card log-in interfaces for multi-factor support. If this software is chosen, both the client and server solution for HP and non-HP platforms must be purchased. The Digital Persona solution is scaleable to hundreds of thousands of users.

Case B: Smart cards and tokens

Smart cards combine two authentication factors - possession and knowledge - and in doing so, provide a higher level of security compared to utilizing only a single factor such as a password. In using smart cards, authentication requires you to be in possession of the smart card and know the secret PIN unique to that smart card. Smart cards are easy to use, providing stronger, portable user authentication on devices and allowing users to authenticate on multiple systems.

Many smart cards and tokens also contain a cryptographic chip/engine which can perform data encryption. Such smart cards can naturally integrate with Public Key Infrastructure (PKI) deployments in a corporation, and provide functionality such as email signing and data encryption.

Note: In addition to PKI support, HP ProtectTools provides the means to more securely store user authentication credentials like passwords; thus does not require added PKI infrastructure elements.

HP offers the HP ProtectTools Java Card. Other smart card suppliers offer separate solutions. Java Card Security for HP ProtectTools is the software module that allows initialization and utilization of the HP ProtectTools Java Card on the PC. However, the smart card keyboard, offered as an AMO for desktop users, and the integrated reader that comes standard in HP business notebooks will support any smart card that conforms to ISO-7816 and has a crypto service provider (CSP).

Like smart cards, USB tokens also combine two factors - possession and knowledge - and can therefore provide a higher level of security compared to authentication devices that use only a single factor. These are convenient and do not require a separate card/token reader as they plug into any open USB port and provide an authentication token similar to the smart card. In addition, some of these tokens come with additional memory that can be utilized for a separate hard drive token. **HP does not currently sell tokens.**

	Security manageability partners		
Customer	**Hardware environment**		**HP Recommendation**
	Exclusive HP	**Multi-Vendor**	
Managed IT	• ActivIdentity	• ActivIdentity	ActivIdentity was the collaborator for development of the HP ProtectTools Java Card and the Java Card Security for HP ProtectTools software. The HP ProtectTools Java Card is ActivIdentity's standard smart card. Their enterprise software version, Enterprise Access Card Solution, can utilize the HP ProtectTools software. Thus, you need not purchase the ActivIdentity client version for HP platforms. ActivIdentity Enterprise Access Card Solution provides enterprise management for both smart cards and tokens.

Case C: All strong password policy with Credential Roaming

Credential Roaming allows you to access various devices in a networked environment with the credentials being retrieved from the server for each session.

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• Bioscrypt	• Bioscrypt	Strong password policy with Credential Roaming is very common and is supported in a single Microsoft Windows ® Domain environment. For implementation of Single Sign On with Credential Roaming in a multiple domain environment, Verisoft Single Sign On from Bioscrypt is the preferred solution as it supports many different credentials including passwords and provides features such as Single Sign On and Credential Roaming.

Scenario 3 - Strong authentication policies w/ enterprise single sign-on in multiple domain environments

This capability enforces stringent authentication policies using biometrics, smart cards, TPMs[1], etc. in multiple domain environments and enables users to easily access secured websites and applications. Personal credentials are kept secure and users are prompted to add new credentials as needed.

Case A: Strong authentication policies w/ enterprise single sign-on and remote biometric authentication

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• Bioscrypt • DigitalPersona	• Bioscrypt • DigitalPersona	• Bioscrypt's Verisoft Single Sign On (Server) was built for multi-factor environments and any combination of biometrics, smart cards, TPMs, etc. and provides features for Single Sign On in a multiple domain environment. • DigitalPersona's solution, DigitalPersona Pro (Server), is built specifically for biometrics and works with Microsoft standard password and smart card log-in interfaces for multi-factor support. If DigitalPersonal Pro is selected, both the client and server solution must be purchased. Digital Persona is scaleable to hundreds of thousands of users.

[1] The TPM (Trusted Platform Module) embedded security chip on select HP's business clients provides the same authentication capabilities as a smart card or token but can be considered a non-portable smart card or token since it is permanently bound to the platform.

Case B: Strong authentication policies w/enterprise single sign-on and remote smart card or token authentication in multiple domain environments

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• ActivIdentity • Bioscrypt	• ActivIdentity • Bioscrypt	• Smart Card or Token only. ActivIdentity was the collaborator for development for the HP ProtectTools Java Card. HP ProtectTools Java Card is a standard ActivIdentity card with additional support built in for HP ProtectTools and pre-OS authentication. ActivIdentity's Enterprise Access Card Solution can utilize the HP ProtectTools software. Thus, the customer need not purchase the ActivIdentity client version for HP platforms. ActivIdentity's Enterprise Access Card Solution will work for both smart cards and tokens but is not extensible for biometrics. • Verisoft Single Sign On by Bioscrypt also supports the remote smart card capability like HP ProtectTools Java Card, and, additionally allows the customer to extend and include biometrics or TPM authentication.

Scenario 4 - Drive Encryption

HP offers Drive Encryption for HP ProtectTools which uses strong access control and pre-boot authentication for both users and platforms to prevent unauthorized access to desktops, workstations, and notebooks PCs. It provides industry-leading full volume encryption with algorithms such as RC5-1024 and AES-256. Encryption and decryption on all storage drives are performed on the fly - transparent to the user - with minimal performance impact and without requiring end-user training. Drive Encryption offers seamless sign on to Windows, secure hibernation, and password rules.

McAfee, HP's security collaborator for Drive Encryption, offers a web service for key recovery which is appropriate for customers with limited IT resources where deployment of an entire infrastructure for drive encryption key management is not feasible. McAfee also offers central manageability for enterprise customers.

Drive Encryption for HP ProtectTools supports smart cards, USB token technologies, and PKI certificates. In addition to password authentication, it provides multifactor pre-boot authentication, which requires users to both "know something" and "have something" before desktops, notebooks or tablet PCs are allowed to start.

Through McAfee's Endpoint Encryption, central management capabilities include central deployment, remote upgrades, mandatory security policy management, a scripting tool, hot revocation, audit facilities, secure centralized recovery, and policy synchronization with Active Directory®, Novell®, PKI, and others.

How does it compare with Microsoft's Vista BitLocker?

Microsoft includes full volume encryption with BitLocker in Windows Vista Enterprise and Ultimate editions. If you are not planning to transition to Vista, you do not have the ability to use BitLocker. Drive Encryption for HP ProtectTools not only supports Vista Enterprise and Ultimate editions, but also extends full volume encryption to include Windows XP and Windows Vista Business/Home.

If you are not using Windows Vista Enterprise or Ultimate edition, Drive Encryption for HP ProtectTools is the clear choice for data encryption. In a managed environment, the enterprise edition by McAfee should be the product of choice.

Both BitLocker and Drive Encryption for HP ProtectTools are viable alternatives. The Drive Encryption enterprise edition, McAfee Endpoint Encryption, has features such as auditability and Help Desk that are not fully developed in BitLocker.

	Security manageability partners		
Customer	**Hardware environment**		**HP Recommendation**
	Exclusive HP	**Multi-Vendor**	
Managed IT	McAfee	• McAfee • PointSec • Utimaco	• HP recommends utilizing the client version of Drive Encryption for HP ProtectTools. McAfee is the recommended vendor for manageability because their offering is scaleable to meet the needs of mid-market and enterprise customers. This is unique to McAfee and one of the reasons HP chose to work so closely with them. • HP recommends McAfee's Endpoint Encryption (enterprise edition) because of its extensive validation testing and preferred pricing on HP systems (the client version is installed on business PCs). This makes a significant pricing differential in favor of HP

	Security manageability partners		
Customer	Hardware environment		HP Recommendation
	Exclusive HP	Multi-Vendor	
			if you require managed drive encryption. • For mid to large enterprises, McAfee's Endpoint Encryption, PointSec and Utimaco all provide drive encryption key management and recovery to meet the needs of the managed IT. These are licensed per client/per seat basis. ***NOTE:*** *If McAfee's Endpoint Encryption software is deployed, it may be necessary to install the client version on HP and non-HP platforms.*

Scenario 5 - TPM

Select HP commercial desktops, workstations and notebooks offer a TPM v1.2 embedded security chip that has been designed in compliance with the Trusted Computed Group specifications. This section will cover enterprise-level TPM initialization and usage models.

Case A: TPM initialization and enablement

HP platforms are delivered with the TPM embedded security chip in a hidden and/or disabled state2 allowing opt-in decision by the IT organization. Prior to using the TPM, the user or IT organization must "take ownership" (per Trusted Computing Specification) of the TPM, establishing owner and user level passwords in the process. In an enterprise environment, it will be necessary to extend this process across the infrastructure in a centrally managed manner. This section covers the solutions currently available to allow the enterprise to remotely perform these tasks on HP business PCs.

Deployment of the TPM includes initialization, inventory, back-up and restore capabilities, and manageability. Further, it allows administrators to monitor inventory of TPM, change TPM owner and user password, back up specific TPM keys for disaster recovery and, in general, manage the TPM.

	Security manageability partners		
	Hardware environment		
Customer	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
Managed IT	•HP Client Automation •HP Client Manager 6.2 •Softex • HP customized scripting through any other management consoles such as MS SMS, Tivoli	• Wave • Softex • Symantec • Customers' own scripting through any management consoles such as MS SMS or, Tivoli	All of these solutions support TPM enablement and initialization with HP Client Automation and HP Client Manager (Symantec based) being lead solutions for TPM deployment on HP client computers. Additionally, customers requiring key management services should consider Wave and Softex as they provide end to end deployment and TPM key management. For those IT departments that have sufficient resources, HP offers WMI / DCOM interface to manage the TPM. IT Departments can customize their own management solution to integrate with other management consoles. HP provides a scripting kit for HP platforms only through the appropriate HP Solutions Architect.

[2] Some governments require the TPM to be disabled for shipment into their country.

Case B: Utilizing the TPM to enhance Drive Encryption

Embedded Security for HP ProtectTools provides key protection for Microsoft's Encrypting File System (EFS) and Personal Secure Drive (PSD) on TPM enabled platforms. The TPM key protection support has been added to Drive Encryption for HP ProtectTools, HP's full volume encryption solution.

Drive Encryption for HP ProtectTools when enhanced by the TPM works only with an Infineon TPM. Likewise, in a multi-vendor environment where the TPM is utilized for key protection for full volume encryption, the vendor may have a dependency on a TPM from specific suppliers. McAfee is currently tied to Infineon TPM on HP platforms.

	Security manageability partners		
	Hardware environment		
Customer	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
Managed IT	• Mcafee	• McAfee • Pointsec (Checkpoint) • Utimaco	• HP recommends McAfee because of its extensive validation testing and preferred pricing on HP systems (with the client version already installed on business PCs). This can make a significant pricing differential in favor of HP PCs if you require drive encryption. • McAfee's Endpoint Encryption, Pointsec and Utimaco all provide drive encryption key management and recovery to meet the needs of the managed IT. These are licensed per client/per seat.

Case C: Utilizing the TPM to enhance Drive Encryption and biometric authentication

Utimaco today supports biometric authentication along with TPM key protection for select non-HP notebooks using the Upek or Atmel fingerprint sensor; Utimaco is not compatible with HP's current fingerprint sensor from AuthenTec integrated in HP business notebooks and available as a USB fingerprint reader after market option for HP business desktops and workstations.

	Security manageability partners		
	Hardware environment		
Customer	**Exclusive HP**	**Multi-Vendor**	**HP Recommendation**
Managed IT		Utimaco's biometric support is only for Atmel and Upek fingerprint sensors, which are not used by HP.	Biometric integration for drive encryption is **not available**. Note: The TPM is utilized to protect the drive encryption key. Note: Vista BitLocker does not offer smart card or biometric authentication.

Case D: Utilizing TPM plus smart card or token authentication to enhance Drive Encryption

HP provides many differentiating capabilities for HP ProtectTools Java Card in addition to its generic smart card capabilities. With the HP Java Card, you can enhance authentication for BIOS pre-boot, VPN, DriveLock, Drive Encryption, Windows/SSO/certificate log ons, RSA, Entrust or one time passwords. Other non-HP smart cards can support many of the same usage models noted above including drive encryption if they provide a PKCS#11 module for the operating system and applications to communicate with the card.

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• McAfee • ActivIdentity	• McAfee • ActivIdentity	HP recommends McAfee and ActivIdentity enterprise solutions. This combination of leading security vendors provides full support for Infineon TPM to enhance the protection of the disk encryption key in conjunction with smart card or token pre-boot for strong authentication.

Case E: TPM-protected VPN access

The TPM, when used to protect access to any cryptographic key and accompanying certificate on the platform, can result in some significantly powerful capabilities, such as VPN deployment solutions. In most companies, the certificate is deposited on an external token such as a smart card providing strong protection for the key validated by the certificate. Smart cards provide mobility guarantees, but there is also a built in cost if they are lost or stolen. Additionally, smart cards only authenticate the user and not the platform being used to gain access through the VPN.

An alternative means to store and protect the certificate is to deposit the certificate on the user's platform and protect the access of the private key using the TPM. The user is still required to provide TPM authentication/password to initiate a VPN session (user authentication). If the VPN-access private key was created in the TPM as a non-migratable key, then a valid authentication to the VPN gateway additionally ensures user is on the same platform that received the VPN access certificate initially, providing multi-factor authentication with inherent guarantees on the platform as one factor, and knowledge of the TPM password being the other factor.

	Security manageability partners		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Enterprise	• HP Consulting & Integration (HP C&I) • Wave • Softex	• HP C&I • Wave • Softex	If analysis of infrastructure, assistance with deployment, or additional security guarantees is required, HP C&I is recommended. Otherwise, Wave or Softex can assist.

Case F: All TPM use cases with key management

Enablement and management of the TPM with management of the owner and user secrets along with all the key material used by the TSS software to protect secrets (data and certificates) must be backed up in a manner that is readily available if the users lose access to their platforms (theft, loss or breakdown or in a roaming environment). Automatic migration and roaming of the key material is a strong requirement for the use of system assets. A business model that requires a kiosk or shared computing model will require strong automatic key roaming capabilities. This requirement applies additionally for thin clients and blade PCs. For non-shared systems, backup access to the key material is required in case of loss or theft.

	Security manageability vendors		
	Hardware environment		
Customer	Exclusive HP	Multi-Vendor	HP Recommendation
Managed IT	• HP • Wave • Softex	• Wave • Softex	Wave or Softex can assist with the implementation.

Scenario 6 – Device control

A basic requirement for securing a computer system is the control of the import and export of data, the major issue being the theft of electronic data and consequential loss of intellectual property and proprietary information. Protection of sensitive data is critical for all businesses, especially in financial, healthcare and government sectors where legal restrictions and requirements are defined, carefully monitored and rigidly enforced. Hazards presented by CD/DVD read/write drives have been understood for some time, but with the vast array of USB memory sticks, personal music players, etc. that can be easily obtained and automatically recognized by Windows systems, the threat is compounded. Loss of data through these external storage media has now been dubbed "Pod Slurping."

With the right software, controlling the access of these devices can be easily resolved. Device Access Manager for HP ProtectTools can control the type of device users can utilize and can restrict usage down to the specific user or group of users at the client level. HP Enterprise Device Manager is the enterprise version and remote manageability extension of the client version.

	Security manageability vendors		
Customer	**Hardware environment**		**HP Recommendation**
	Exclusive HP	**Multi-Vendor**	
Managed IT	• HP Enterprise Device Manager	• HP Enterprise Device Manager	Device Access Manager for HP ProtectTools is available as a web downloadable feature for HP business notebooks and desktops or is available as an after market option for select business desktops and workstations. For European customers requiring enterprise management of the various users/devices that can be restricted, HP Enterprise Device Manager, delivered by HP C&I in Warrington, UK, allows for central management and policy enforcement. This enterprise manageability offering is available worldwide; at this time, a worldwide SKU is being established which should quickly be available for all ordering systems.

Glossary

Glossary	
3PO (third party option)	Offering available through from HP vendor
Altiris	Business unit of Symantec specializing in management software
AMO (after market option)	Offering available for ordering separate from the platform
CTO (configure to order)	Ordering process by which customers can specify specific features and options to be included with each platform
Drive Encryption for HP ProtectTools	2007 module that provides client version of full volume encryption for one or multiple hard drives. Enterprise class manageability software available from McAfee
Entrust	Security company that provides solutions for PKI, multi-factor authentication, fraud detection, etc.
File & Folder Encryption	Capability to encrypt data on individual files or folders
Full Volume Encryption	Capability to encrypt data on an entire hard drive partition (volume)
HP BTO (HP Business Technology Optimization)	HP business unit specializing in enterprise management software – formerly called HP OpenView
HP Client Automation	HP Software developed management console of client computers for asset inventory, Soft Pack distribution and alert management
HP Client Manager	HP and Symantec jointly developed management console of client computers for asset inventory, SoftPaq distribution and alert management
HP SSM (System Software Manager)	Tool for deployment of SoftPaqs and BIOS updates
Microsoft EFS (Encrypting File System)	Microsoft software that provides file and folder encryption of data. Comes standard with Microsoft Windows 2000, XP or Vista OS.
Microsoft SMS (System Management Software)	Microsoft's client management Systems management software product by Microsoft for managing large groups of Windows based computer systems.
Multi-factor Authentication	Utilizing combination of factors such as biometrics, smart card, etc. for authenticating user logon
Personal Secure Drive	A virtual encrypted disk hosted on any fixed hard drive. The Virtual Drive appears as a separate entity to the user and can be as large as user is allowed to allocate on the entire hard drive, less 5GB to ensure Windows has needed "headroom" space
PKCS#11 (PKCS: Group of Public Key Cryptography Stds)	#11 – An API defining a generic interface to cryptographic tokens
PKI (Public Key Infrastructure)	An arrangement that binds public keys with respective user identities by means of a certificate authority or CA
RSA	Describes a host of Public Key encryption and general encryption algorithms for the computing industry used for e-commerce, SSL, email signing/encryption, etc. RSA is also the name of the company that developed these algorithms.

Glossary	
SSO (Single Sign On)	Serves as a password vault for accessing secured websites and applications.
SafeBoot	Division of McAfee. SafeBoot's Device Encryption software is now entitled McAfee's Endpoint Encryption
Tivoli (division of IBM)	Specializing in infrastructure and service management tools
TSS (Trusted Computing Group software stack)	Software stack that interfaces between the TPM driver (Windows 2000 and XP) and application level software for Windows 2000 and XP. In Vista the TSS interfaces between Microsoft's TBS API level and application software. Embedded Security for HP ProtectTools software acts as TSS and TPM configuration application on HP business PCs.
Vista BitLocker	Microsoft's Vista full volume encryption software – available on Vista Enterprise and Ultimate editions as well as on Windows 2008 Server

For more information

HP

- HP ProtectTools security software suite web ordering: http://h10010.www1.hp.com/wwpc/us/en/en/WF06c/A10-51210-70779-3245603-70779-3676679-3676680-3676682.html
- Security Website: HP Business PC Security http://www.hp.com/products/security
- Notebook Security http://www.hp.com/sbso/solutions/pc_expertise/professional_innovations/protecttools.html
- Desktop Security http://www.hp.com/sbso/solutions/pc_expertise/great-desktops/index.html

Drive Encryption

SafeBoot® / McAfee

- General website: http://www.safeboot.com/
- Fact sheet: http://www.mcafee.com/us/local_content/datasheets/ds_mcafee_endpoint_encryption.pdf

Device Access Manager for HP ProtectTools

HP

HP ProtectTools Device Manager

- General website: www.hp.com/hps/security/products
- Fact sheet: http://h71028.www7.hp.com/ERC/downloads/4AA1-1372EEE.pdf

Multifactor Authentication

Bioscrypt

- General website http://www.bioscrypt.com
- White Paper VeriSoft Single Sign On: http://www.bioscrypt.com/products/verisoft_sso

DigitalPersona

- General website http://www.digitalpersona.com/
- Fact sheet: http://www.digitalpersona.com/products/business.php

Softex Incorporated

- General website http://www.softexinc.com/main.asp

ActivIdentity

- Website http://www.actividentity.com/solutions/technology/sa__overview.php
- Technology Brief on ActivIdentity solutions for Device and Credential Management http://www.actividentity.com/solutions/docs/briefs/AI_device_credential_management_L.pdf

Client Manager and TPM

HP

- Website for HP Client Automation: http://www.hp.com/go/client

Symantec

- General website: www.altiris.com
- Website on HP/Symantec collaboration http://www.hp-altiris.com/
- White Paper: HP/Symantec security offerings http://www.altiris.com/upload/altiris_security_offerings_for_hp_24apr07.doc

Wave

- General website: www.wave.com
- White Paper Embassy Trust Suite: http://www.wave.com/products/ets.asp

Call to action

Contact your HP representative to discuss how you can proceed with implementation of HP security and security manageability for your business.

4AA0-8657ENW, May 2008

invent