Technical Whitepaper

HP Client Security

Commercial Managed IT Software

Contents

Executive summary

This white paper is intended for IT staff. The paper contains sections describing:

- HP's strategic approach to Security
- A description of *HP Client Security* (formerly known as HP ProtectTools), the application that consolidates HP security features so the user can set up and modify all the configurable HP security features available on their HP Business PC.
- A high level overview of the software applications HP uses to support this strategy
- An in-depth look at the *HP Client Security* features.
- Overview on how you can manage certain features of HP Client Security

System requirements and prerequisites

Information regarding minimum hardware requirements for the installation of Windows is available at http://www.microsoft.com.

Supported operating systems

- Windows 7
- Windows 8.x

Supported hardware options

- Smart Card readers
  - Windows: All PKI Smart Cards supported via a PKCS11 or CSP stack.
  - BIOS: None
  - Drive Encryption: ActivIdentity Cyberflex Access 64K V2c
- Fingerprint readers
  - Validity fingerprint readers VFS 471, VFS 491 and VFS495 in secure mode
- Omnikey readers
  - Contactless HID iCLASS memory cards
  - Contactless MiFare Classic 1k, 4k and Mini memory cards
  - HID Proximity cards
- Bluetooth® phone
  - iOS
  - Microsoft Windows
  - Android™
- DigitalPersona Fingerprint sensor integrated on Elitepad Security Jacket
  - FIPS 201 certified
  - HP ProtectTools Security Manager V8.0 or greater required.

Pre-requisites

- Microsoft .Net Framework 3.5, 4.5
- Windows Installer MSI 4.5
- Microsoft Visual C++ Redistributable 2008 and 2010

Introduction

HP's decorated history in personal computer security has been based on the belief that security should be built in and not bolted on. This belief has led to the development of *HP Client Security* (formerly known as HP ProtectTools); the specially developed multi-layered, hassle-free enterprise-level Windows application. It is the reason why HP includes *Client Security* on Business Desktops, Notebooks and Workstations. HP believes that PCs should not become points of vulnerability that threaten an entire infrastructure. Instead they should be trusted, easy to use, extensible and manageable.

Rather than simply installing third-party software to satisfy a requirement, HP innovation also extends with chosen software partners to design software that is optimized for HP hardware. Each security software solution receives thousands of hours of development, validation, and quality assurance.

As a part of the HP holistic approach, HP Client Security is built into the BIOS, hardware, and software layers. HP plans to continue our rich heritage in enterprise security; while maintaining an advantage over the competition by consistently adding new security features desired by customers.

HP Security Strategy

The HP security strategy to protect users is encompassed through:

- Data Security (Shown in Table 1)
- Device Security (Shown in Table 2)
- Identity Security (Shown in Table 3)

HP believes these areas of protection cannot be accomplished with only bolted on solutions. This is why HP ensures that security is built-in to the PC in all three layers:

- BIOS - HP BIOSPhere integrates many security features at the core of the PC.
- Software – HP Client Security software features.
- Hardware – Vetted out security related hardware modules.

These multiple protection points guard against security attacks, loss or theft. As a result, HP Business PCs can defend businesses and users conveniently. HP *Client Security* helps you meet compliance requirements with thoroughly tested comprehensive, multi-layer features that are easy to deploy and manage. Tables 1, 2, and 3 below provide a list of features for each of the three layers falling under Data, Device, or Identity. The following paragraphs provide a more complete description of each feature.

Table 1 Data Protection Security Features

Layer	Data protection	Description
BIOSphere[1]	HP DriveLock[2]	Protects your hard drive data by not allowing it to operate unless you enter the appropriate password when the system is turned on. DriveLock supports both Self-Encrypting and standard hard drives.
	HP Automatic DriveLock[3]	With Automatic DriveLock the BIOS provides the password when the system is turned on. This prevents the drive from being used in another system unless the BIOS Administrator passwords match.
	HP Disk Sanitizer[4]	Allows you to permanently destroy data on the hard drive prior to redeployment or system disposal. Unlike hardware-based Secure Erase (See Secure Erase on page 6), Disk Sanitizer is a software solution that rewrites the entire drive. Only traditional hard drives are supported by Disk Sanitizer.
Software-based	HP Drive Encryption [5] (See HP File Sanitizer on page 144)	Drive Encryption software encrypts all information on a hard drive (HDD or SSD) volume so that it becomes unreadable during unauthorized access. Starting with new 2013 PCs, HP Drive

Layer	Data protection	Description
		Encryption is FIPS 140-2 L1 certified. • With Drive Encryption, authentication (a password, smart card or fingerprint) is required before Windows will even start • Encrypted drives removed from the system cannot be read by another PC without proper authorization • HW encryption supported with Self-Encrypting Hard Drives (SEDs). • HP Drive Encryption provided with new 2013 PCs is powered by WinMagic. 1. For enterprise level manageability, HP Drive Encryption is upgradeable to WinMagic SecureDoc Enterprise. HP offers licensing for HP and non-HP PCs. 2. For HP Drive Encryption on PCs released prior to 2013, DigitalPersona Pro Workgroup offers enterprise level manageability.
	HP File Sanitizer [6] (See HP File Sanitizer on page 21)	You can permanently erase individual files, folders and personal information from the internal hard drive on your PC. Only supports traditional hard drives.
	HP Trust Circles [7] (See HP Trust Circles on page 22)	HP Trust Circles protects accidental data leakage by allowing only members of a Trust Circle to access specified documents. Assign folder(s) to each Trust Circles, and all files placed in those folders are encrypted so that only the contacts assigned to the Trust Circle can access them. • When included, HP Trust Circles Standard supports creating up to 5 Trust Circles with up to 5 contacts per Trust Circle.
	HP Disk Sanitizer External Edition	Software that will permanently destroy data on standard hard drives in preparation for system disposal or redeployment. A printable report is generated for this operation.
	HP Privacy Manager [8] (End of Life)	Protect supported Microsoft Office® files and emails sent in Microsoft Outlook® by allowing only your selected Trusted Contacts to access the information. • Creates a digital identity that is verified by authentication to help prevent supported Microsoft Office files from getting into the wrong hands by encrypting for selected trusted contacts only • No longer offered with new HP Business PCs. Check product data sheet.
Hardware-based	Common Criteria EAL4+ Certified TPM	A Common Criteria certification Evaluation Assurance Level 4+ (EAL4+) Trusted Platform Module (TPM) provides hardware-based encryption keys and more secure storage.
	Self-Encrypting Drives (SEDs)	Encrypts and decrypts data as it is being written to, or read from the drive. Users get faster encryption performance than that of software-based only encryption solutions.
	Secure Erase [9]	Permanently destroys data on your hard drive (HDD or SSD) in preparation for system redeployment or disposal. Once executed, the hard drive controller will completely rewrite all the data on the drive and cannot be recovered even with advanced data recovery tools. Meets NIST 800-88 Secure Erase guidelines.

1. HP BIOSphere features may vary depending on the PC platform & configuration.
2. Self Encrypting HDs (SEDs) are not supported if the encryption PIN is enabled.
3. Automatic DriveLock will work on another HP Business PC when the BIOS passwords are the same. Requires user set up.
4. For the use cases outlined in the DOD 5220.22-M Supplement. Does not support Solid State Drives (SSDs). Requires Disk Sanitizer, External Edition for Business Desktops from hp.com. Requires Windows on business desktops and notebooks..

5. Requires Windows. Data is protected prior to Drive Encryption login. Turning the PC off or into hibernate logs out of Drive Encryption and prevents data access

6. Requires Windows. Data is protected prior to Drive Encryption login. Turning the PC off or into hibernate logs out of Drive Encryption and prevents data access.For the use cases outlined in the DOD 5220.22-M Supplement. Does not support Solid State Drives (SSDs). Initial setup required. Web history deleted only in Internet Explorer and Firefox browsers and must be user enabled. With Windows 8.1, user must turn off Enhanced Protection Mode in IE11 for shred on browser close feature.

7. Windows required. When included, HP Trust Circles Standard allows up to 5 Trust Circles with up to 5 contacts in each Trust Circle. HP Trust Circles Pro required for unrestricted number of Trust Circles and contacts. HP Trust Circles Reader is available to allow a contact to participate in an invited Trust Circle. Available at http://hptc.cryptomill.com. Trust Circles is available only on select products. Please consult the product's data sheet for more information.

8. Requires initial setup and Microsoft Outlook and Microsoft Office. One year of service included. For users without HP Privacy Manager, DigitalPersona Privacy Manager is required for sharing encrypted files and emails, and six months of service is included. Users can use their own compatible digital certificate instead of offered service.

9. For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88. ElitePad 900 G1 support with BIOS F.03 and higher.

Table 2 Device Protection Security Features

Layer	Device protection	Description
BIOSphere	HP Sure Start[1]	HP Sure Start is the first and only self-healing technology solution created to protect against Malware and Security attacks aimed at the BIOS, developed in collaboration with HP Labs. Sure Start is a hardware based solution that protects and recovers the BIOS Boot Block regardless of the cause of corruption or compromise assuring a virtually un-interrupted boot. Sure Start is independent of CPU such that any virus or malware is not aware of Sure Start or any of its components making this a technology not easily susceptible to attacks.
	HP BIOS Protection [2]	Developed according to NIST SP 800-147 security guidelines, this feature protects the BIOS from attacks. All BIOS updates are checked for a proper cryptographic signature. If this check fails, the platform will refuse the update. • If malware is able to circumvent this process, and malicious code is detected, the BIOS repairs itself using a verified BIOS copy that is stored in the system flash memory or in the HP_Tools partition. Otherwise, the system does not boot and emits a particular LED code. Users can recover manually by flashing the BIOS from a USB storage device.
	Pre-boot Security	Built-in security features such as BIOS security, port control, communications device control, boot options, and Absolute Persistence module.
	Absolute Persistence[3] **(See** Absolute Data Protect (ADP) on page 31)	Once subscribed and activated to supported Absolute services (purchased separately), the Persistence Module ensures that activated Absolute software services, like Computrace have their agent replaced in Windows, if it is ever removed. For more information visit http://www.absolute.com/ .
	Master Boot Record Security	Backup and then restore your MBR if it gets compromised. Business Desktops BIOS can additionally lock the MBR so that it cannot be written to while locked.
Software-based	HP Device Access Manager with Just in Time Authentication (See HP Device Access Manager (HPDAM) on page 19)	Provides advanced security options to selectively block ports, connections, and storage devices that can compromise the security of your PC or your network. • Allows an Administrator to define which users or groups have access to which devices that are connected to or integrated into the PC. • Prevents someone from walking up to your unlocked PC and taking data off your computer onto a USB Drive • Just In Time Authentication allows data transfer to Removable Storage (ex. USB Drives) or Optical Disk Drives

Layer	Device protection	Description
		for a brief period of time only after the user validates their identity.
	Absolute Data Protect[3] **(See** Absolute Data Protect (ADP)on page 31)	Enables you to manage your PC remotely with remote Find, Lock, or file Erase. • 4 years of service included in the ElitePad 900 and Windows 8 EliteBook Revolve 810 • Upgrade to LoJack for theft recovery available when the user logs into my.absolute.com to manage their account
	Microsoft Security Essentials (Win7) / Microsoft Defender (Win8.x) [4]	Prevents and detects most malware attacks from compromising a PC, not based on subscriptions that can expire.
Hardware-based	Physical device security: chassis security kits, locks, cables, and sensors	HP supports a variety of accessories to protect against physical loss of a device and its hardware components.

1. Supportedon select products only, see product data sheet.
2. For PCs without a backup copy in the system flash memory requires an HP_Tools partition for automatic recovery. Feature not supported on Business Desktops released prior to 2013 nor ElitePads, see product data sheet.
3. Absolute agent is shipped turned off, and will be activated when customers activate a purchased subscription. Subscriptions can be purchased for terms ranging multiple years. Service is limited, check with Absolute for availability outside the U.S. The Absolute Recovery Guarantee is a limited warranty. Certain conditions apply. For full details visit: http://www.absolute.com/company/legal/agreements/computrace-agreement. Data Delete is an optional service provided by Absolute Software. If utilized, the Recovery Guarantee is null and void. In order to use the Data Delete service, customers must first sign a Pre-Authorization Agreement and either obtain a PIN or purchase one or more RSA SecurID tokens from Absolute Software. Absolute Data Protect requires the user to activate the included subscription.
4. Internet access required. Opt-in is required to receive updates.

Table 3 Identity Protection Security Features

Layer	Identity protection	Description
BIOS Security	Power-on Authentication [1] (See HP Client Security – Manageability Options on page 9)	Requires users to authenticate themselves when turning on the computer before the operating system or any other software will start. HP Business Notebooks support the users' Windows Password or Fingerprint, and Business Desktops support a separate password that requires setup in the BIOS
	Enhanced Pre-boot Security	HP Business Notebooks provide additional pre-boot security capabilities, consisting of multiple users in the BIOS identified with their Windows credentials, fingerprint reader reset, HP One Step Logon and HP SpareKey support.
Software-based	HP Credential Manager [2] (See HP Client Security – Manageability Options on page 9)	Supports multiple authentication methods and two-factor authentication policies: • Windows Password • Integrated Fingerprint Reader sensor (Business notebook option) • Smart Card* (CSP, PKCS11 standards) with integrated Smart Card reader or Smart Card keyboards • Contactless / Proximity Card* (HID iCLASS and Proximity, MiFare Classic 1K, 4K, and Mini) with supported card readers (OMNIKEY readers, e.g. 5321, 5325) • Bluetooth (mobile phone device) • PIN • Face Recognition (Win7 business PCs released prior to 2013)

Layer	Identity protection	Description
		*Cards and middleware required and not included.
	HP Password Manager [3]	Allows a user to conveniently use unique usernames and passwords for websites and applications. After the user identifies themselves with any enrolled credential, Password Manger enters the appropriate account information on their behalf.
	HP SpareKey [4] (See HP Client Security – Manageability Options on page 9)	Allows users to securely log into their PC if they forget their password, lose their smart card, or cannot use their fingerprint to login. • Supports custom SpareKey questions in addition to the 10 pre-defined questions. • Eliminates the need for the end user to call the Help Desk to reset their password. • When used, HP SpareKey will start the Windows password reset process. • HP Business Notebooks support HP SpareKey with BIOS, HP Drive Encryption, and Windows. • HP Business Desktops support HP SpareKey with HP Drive Encryption and Windows.
	HP One Step Logon [5]	Authenticate once at the first login prompt and the PC will continue booting the user through Windows login without requiring any additional authentication. • On HP Business Notebooks One Step Logon supports Power-On Authentication, HP Drive Encryption, and Windows. • On HP Business Desktops and Tablets, One Step Logon supports HP Drive Encryption and Windows.
	HP Face Recognition (End of Life)	Use an integrated or attached webcam to identify authorized users by their face. Enhance security by pairing with your Bluetooth phone or to a PIN. • Supported on Windows 7 business PCs released prior to 2013
Hardware-based	Smart Card Readers	An ISO7816 standards-based Smart Card Reader is an integration option for HP Business Notebooks. Smart Card Keyboards are available as an HP accessory option for HP Business Desktops. All Smart Card readers are FIPS 201 compliant.
	Fingerprint Reader Sensor	The integrated swipe Fingerprint Sensor on HP Business Notebooks is isolated hardware that is highly spoof-resistant, very secure, does the match of the fingerprint on the sensor, and creates fingerprint templates rather than storing fingerprint images. • The Fingerprint Sensor included on the HP Security Jacket is a FIPS 201 certified touch sensor.

1. Not supported on the ElitePad 900 G1.
2. Requires Windows. User setup required.
3. Requires Internet Explorer (IE) some websites and applications may not be supported. Supported in"Desktop Mode" on Windows 8.x. Some browsers require the Password Manager extension to be enabled by the user. Not compatible with Internet Explorer with Enhanced Protected Mode enabled.
4. Requires initial user setup. Business desktops and ElitePads do not support SpareKey in BIOS.
5. HP Business Desktops do not support One Step Logon with BIOS Power-on Authentication. One Step Logon does not support Power-on Authentication with the TPM. One Step Logon is disabled in Windows when software Secure Attention Sequence is enabled by Windows Group Policies.

HP Client Security – Manageability Options

HP Client Security has multiple management options:

- Local Management - HP Client Security application allows for full policy configuration.
  - Limited users may not change policies.
  - Policies can be set in an image before deployment.
- HP Credential Manager cloud-based remote management - DigitalPersona offers Pro Workgroup SaaS
  - Access Recovery, credential policies, HP Drive Encryption (for HP Business PCs launched prior to 2012), and centralized reporting
  - 5 licenses are available for testing/pilot
  - Visit www.protecttools.com for more details
- HP Drive Encryption– upgrade to WinMagic SecureDoc Enterprise for remote management.
  - HP offers licensing for HP and non-HP PCs.
  - Contact your HP Sales representative or reseller as well as Visit www.winmagic.com/hp for more details
- BIOS remote management
  - Most features are managed remotely by optional LANDesk management software., HP BIOS Configuration Utility and other management consoles.
  - Visit www.hp.com/go/clientmanagement for more details.

Remote Management Alternatives to HP Client Security Technology

- HP Enterprise Device Access Manager
  - It provides similar functionality to HP Device Access Manager but with centralized manageability.
  - Offers administration tools to define and maintain the device access control policy which is stored in Windows Active Directory.
  - Does not support Just In Time Authentication
  - Visit www.hp-protecttools.com/products.asp
- SEAHawk
  - SEAHawk provides similar capabilities to HP Trust Circles, allowing IT to determine Trust Boundaries for users and integration into Active Directory
- Contact your HP sales representative for more information.

HP Client Security Technology

HP Client Security consists of the following key security technologies:

Security and Encryption Strength

HP Client Security's core host application adheres to a strong security model with the following features:

- Execute all "secure operations", such as, user authentication, user provisioning, credential management, and policy configuration from a highly privileged account.
- Use Windows ACLs (Access Control List) to protect access to resources, such as registry data.
- Generate a PKI key pair to be used by the authentication service in conjunction with cryptographic functions.
- Generate the PKI and symmetric keys (UUK) upon enrolling a user. The UUK is not stored in the clear or simply obfuscated on the hard drive. The key is always protected via a credential. User's Windows password is used to derive a key that is then used to encrypt the UUK. Additiionally, the key is either encrypted as with the Smart Card or securely stored in the authentication device as with the secure fingerprint reader. The UUK is only released upon a successful user authentication. This key in turn encrypts other sensitive user data, the so called "user secrets". In the end, the secrets are always protected via user authentication.
- Microsoft Enhanced Cryptographic Provider (ECP).

Design and Services

HP Client Security provides an authentication service to ensure that the user authentication capabilities extend beyond Windows, and that BIOS and Drive Encryption login pages can participate in user authentication as well. All communication between the authentication service and authentication environments occurs at the service layer. The authentication service provides the following functionalities:

- Manages the activation and deactivation of the authentication environments (Windows, BIOS, Drive Encryption).
- Coordinates the authentication policies and user provisioning data across all authentication environments, thus facilitating One Step Logon and ensuring that a lockout scenario is avoided.
- Enroll users' credentials.

HP Client Security - Setup Wizard

The HP Client Security setup wizard helps secure access to your computer via a password, a fingerprint sensor (if available), or the HP SpareKey if a password or other credential is lost. The wizard safeguards hard drive access and data using HP Drive Encryption for robust information protection. It ensures that removable media cannot be accessed until authenticated with HP Device Manager with Just-In-Time Authentication, and even then the access is granted for a limited time. The wizard also enforces the default setting of Windows logon authentication and places the HP File Sanitizer icon on the desktop.

HP Client Security offers a one-time wizard shown in Figure 1, which guides a user through the setup of core security features that include:

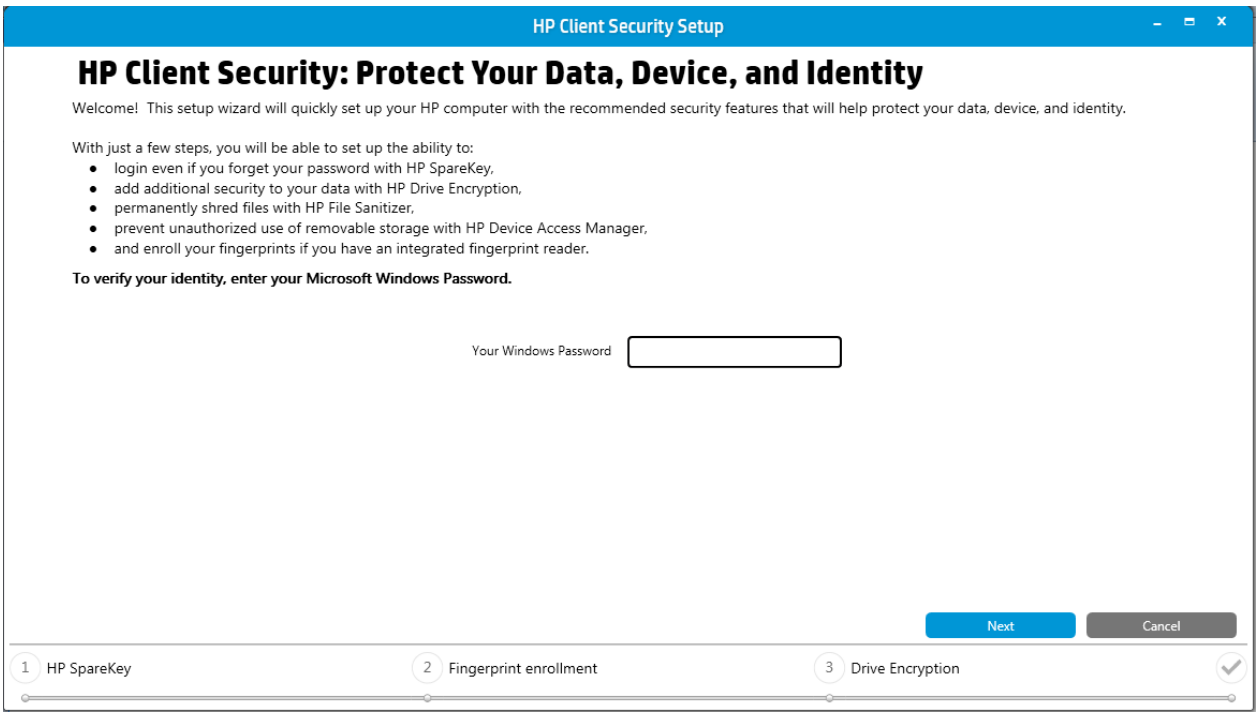

Figure 1 HP Client Security Setup Wizard

- Password authentication
  - Prompts user to verify their identity by typing their Windows password. This prevents other users from setting up the system using another person's account.
  - Requires user to create a Windows password if one doesn't already exist.
  - Rejects passwords that contain invalid characters such as those that cannot be supported by HP BIOS.
  - Displays password strength advice when creating a password.
  - Enables HP Client Security to be able to log the user into Windows.
- SpareKey enrollment
  - Allows the user to login to Windows by answering 3 security questions instead of a password (if forgotten) or other credential (if not available).
  - Rejects answers containing invalid characters that cannot be supported by HP BIOS.

- Allows only English, French, Italian, and German characters for Security questions and corresponding answers.

- Fingerprints enrollment (only shown with supported fingerprint readers)
  - Requires enrollment of two fingerprints. If needed, a user can enroll additional fingerprints later using the HP Client Security application.
  - Enrollment process starts immediately upon the user swiping their first finger.
  - Allows the user to login to Windows with their fingerprints.
  - To enroll a finger, the user provides a few good quality finger scans for each finger.
  - Reflects fingerprint enrollment process in a progress bar.
  - Uses lower text area to provide feedback or guideline to the user.
- Drive Encryption activation (if installed)
  - Automatically selects the primary system partition to be encrypted if the user does not skip this feature enrollment.
  - If primary disk is an Opal self-encrypting drive (SEDs) then it will perform hardware encryption automatically.
  - User must select the encryption recovery key back-up mode. The user can choose Removable Media and/or SkyDrive.
  - HP Drive Encryption uses TPM protection for drive encryption, if initialized and owned.
- Just In Time Authentication (JITA) activation
  - By completing the wizard, it sets a default policy where access is allowed to all devices for all users, except for removable storage where JITA access is required with a 15 minute duration.
- File Sanitizer
  - Completing the wizard, places the File Sanitizer icon  on the desktop to allow a user to drag files or folders to the icon in order to securely delete them.
- The Finished page provides a summary of the settings and credentials set up by the user. It also provides information about aditional features of the HP Client Security product.

NOTE

The changes are saved on the wizard on a page-by-page basis. If for example, the user enrolls their fingerprints, but cancels the wizard in a later page, the fingerprint enrollment is still successful and enrollment data has been saved.

HP Client Security - Application

HP Client Security can be accessed from a single, console interface icon in the Windows® task bar, the system tray, the Control Panel, the Windows 7 Start menu, a Windows 7 desktop gadget, or Windows 8 start page. The HP Client Security home page shown in Figure 2 is the central location for easy access to HP Client Security features, applications, and settings.

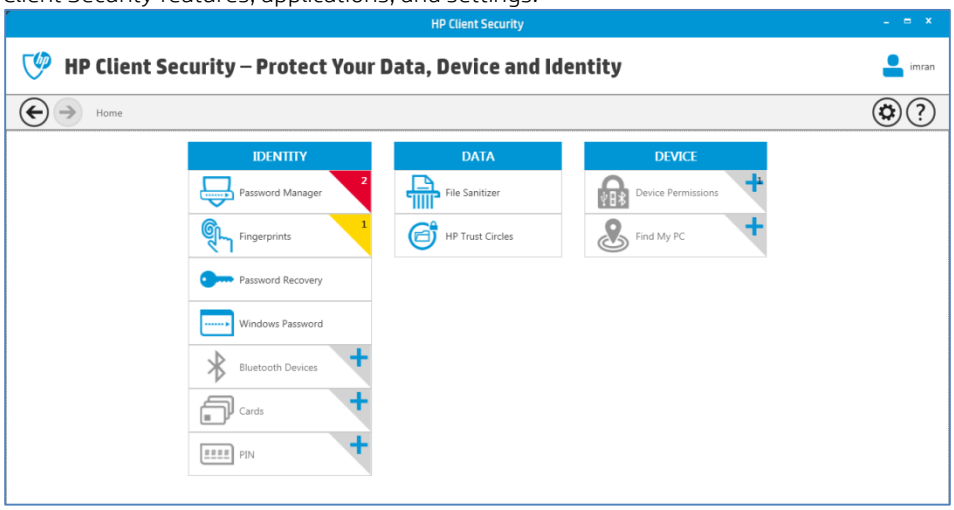

Figure 2 HP Client Security Home Page

The Home page is divided into three sections:

Identity	Provides Credential Manager features of enrollment and management of authentication credentials (password, fingerprint, cards, Bluetooth, PIN, and HP SpareKey) and ability to access Password Manager in order to add/edit/manage logon data for websites and applications.
Data	Provides access to applications used for managing data security – HP Drive Encryption, HP File Sanitizer, and HP Trust Circles.
Device	Provides access to applications used for managing device security – HP Device Access Manager, HP Computrace.

Additionally, *HP Client Security* provides access to Advanced Settings gear icon at the top right in order to configure administrators and standard user's policies for both logon and session; manage PC users; activate or deactivate Windows and power-on authentication; and backup or restore HP Client Security data (primarily Password Manager).

For added security, user authentication is enforced and all administrative level configuration operations require Windows UAC elevation.

User Management

Accessing the User Management page shown in Figure 3 from the Advanced Settings icon allows you to create and delete HP Client Security users in a system wide manner. To ensure users and security policies are synchronized between the operating system and the pre-boot environment, users should always be added and deleted using HP Client Security user management.

Selecting a user icon on the Users page will launch an authentication policy summary for that user – it will display credentials and policies as configured by/for that user. Selecting a credential will allow its enrollment.

"Login policy" applies to the Windows Logon. "Session policy" applies to security applications running in Windows that leverage Credential Manager, such as Password Manager.

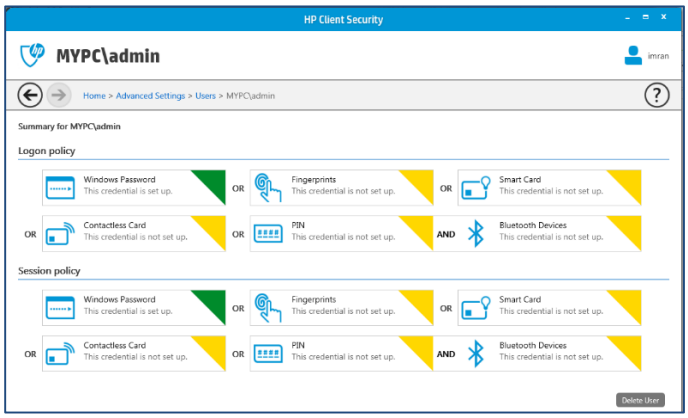

Figure 3 HP Client Security User Management

Policies

The Administrators Policies window shown in Figure 4 provides the ability to configure login and session policies for the applicable user(s). The Standard Users Policies has a similar interface. Logon policies govern the credentials required to log on to Windows. Session policies govern the credentials required to verify identity within a Windows session, such as with Password Manager, Trust Circles, and Just In Time Authentication.

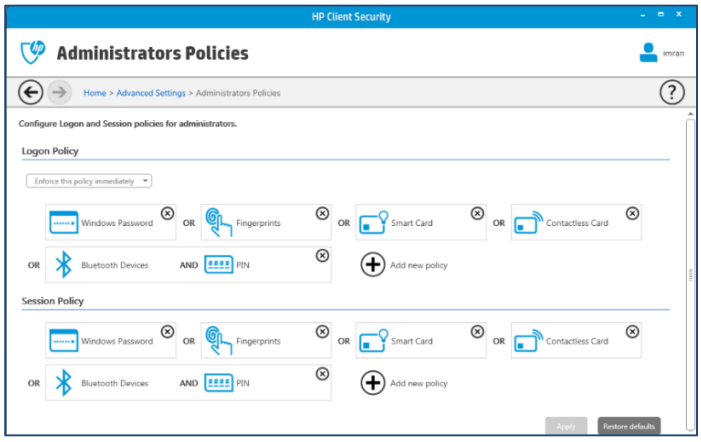

Figure 4 HP Client Security Logon & Session Policy Configuration

You can control authentication strength to increase system security by requiring user to authenticate with more than one credential or with specific credentials only when available.

The authentication logic is as follows:

- OR: User can enter either one of the two credentials to authenticate. User may select individual credentials for authenticating, such as Password OR Fingerprint.

- AND: User is required to enter both credentials to authenticate. The user may select a combination of 2 credentials for authenticating such as Bluetooth AND PIN.

When defining a logon or session policy, a credential configured as part of the AND logic cannot be selected with the OR logic.

Password Manager

Password Manager provides the ability to automatically remember and then supply credentials for websites, applications, and protected network resources. Password Manager includes a personal password vault that makes accessing protected information more secure. Password Manager protects the data with encryption and an Access Control List (ACL).

Key features of Password Manager include:

- Checks the strength of individual passwords used for websites and applications when adding login data.
- Allows creating stronger passwords without the need to have to write them down or always remembered.
- Log on easily and quickly with a finger swipe, or with another credential, such as, Smart Card, proximity card, contactless card, Bluetooth phone, PIN, or your Windows password.
- Works with 2-factor authentication capabilities to add additional protection during authentication.
- Imports web logon data from or exports it to the supported browser vault.
- Categorizes accounts for better organization.
- Allows an account to be marked as compromised. User will then be able to see at a glance whether any of the other accounts share the same password and also would have been considered compromised and are a security risk.
- Detects if a login to a new website has occurred, or if a login was different than what is stored in Password Manager. During this event, Password Manager prompts the user to remember the new or updated login information.
- The following browsers support Password Manage :
    - Internet Explorer (IE) - Import and export features not supported in IE 10 and 11, User may need to disable Enhanced Protected Mode in IE 11 for Password Manager plug-in to work.
    - Chrome -May require a user to enable the HP Client Security add-on before Password Manager feature will start to work.
    - Firefox - May require a user to enable the HP Client Security add-on before Password Manager feature will start to work.

Backup and Restore

To back up Password Manager login credentials click the 'Advanced Settings' icon to access HP Client Security Backup and Restore. This is not a user data backup solution. HP Client Security Backup and Restore:

- Requires creation of a password for the backup file in order to prevent it from being restored by another user. The backup file can be saved on the PC or SkyDrive.
- By default, once installed and signed in, a SkyDrive folder will be created in the …Users\<accountname>SkyDrive folder, and SkyDrive will appear in your Favorites folder in Windows Explorer.

The backup data can be restored to the same or another PC protected by HP Client Security from the PC or SkyDrive by entering the required password for the backup file

Validity Fingerprint Reader Sensor/Driver (VFS495)

Technology

- The VFS495 meets the requirements of FIPS140-2, but is not FIPS 140 certified.

The VFS495 uses the following encryption and data security technologies:

- Advanced Encryption Standard (AES) hardware block - Encrypts/decrypts data stream with AES-CBC-256 and RSA-2048. AES cryptography is performed in CBC mode.
- Hardware exponentiation block - Performs RSA operations.
- Security Hash Algorithm (SHA) hardware block - Calculates SHA1/256, SHA1/256-HMAC on data stream
- Physical Unclonable Function (PUF) – two PUF hardware blocks 224 bits each - Generates unique 448 bit output for each VFS sensor, used to generate key material.
- One Time Programmable) Memory (OTP) - 1 Kbit OTP memory inside the sensor used to store security and sensor configuration data.
- Random Entropy Source - Noise data from Sensor (analog block) is used as the main source of entropy. Additionally, CPU clock cycle count can be used to mix up for better entropy.
- Secure Sockets Layer (SSLv3) - Communication between the Validity SDK and the sensor are encrypted using SSLv3. The RSA and AES algorithms and SHA and MD5 operations are used in the SSL Handshake and communications to authenticate parties, to generate shared keys and secrets, and to secure communications.

All firmware patches for VFS-RSA sensor will be AES-CBC-256 encrypted and RSA-2048 signed before deployment. The sensor firmware verifies the RSA signature before accepting a patch.

Design

The following Validity fingerprint solution embedded security features relate to the HP Client Security, including BIOS and Drive Encryption:

- A HP-signed DLL for use by HP Client Security.
- A Validity service.
- A WinUSB device driver.
- Secure delivery of fingerprint image.
- A protected channel for secure communication between Host and Sensor.
- A unique RSA-2048 public/private key pair for every sensor.
- A unique, random AES-256 key for template database encryption that is invalidated and re-generated on device ownership change.
- Sensors can authenticate a Host and be authenticated by a Host
- SecureMatch® - the ability to verify match results on the sensor before any user payload data or credentials are released to the host.
- Provides a Unified Extensible Firmware Interface (UEFI) driver that the BIOS or Drive Encryption environments can call to implement single-sign on a matching finger swipe.
- The UEFI driver only releases the SID on an authenticated SecureMatch®.
- Securely extendable firmware for supporting One Time Password (OTP) solutions.

- Embedded Secure Template Database will securely protect application-provided user payload data / user credentials bound to the finger enrollment.
- Up to 50 finger enrollments may be stored in the secure database, beyond this, fingers must be removed before new enrollments can be performed.
- The following items are included in the manageability scheme for the fingerprint reader:
    - Min/max finger enrollment count.
    - Fingerprint matcher threshold (convenience vs. accuracy adjustment).
    - Power management
    - Fingerprint reset
        - Marks the information in the sensor to be overwritten. All fingerprints must be re-enrolled.
        - NOTE: Secure hardware fingerprint reader reset is available in F10 Computer Setup. Ensures that all trace of biometric data are eliminated by completely erasing the Flash memory and laying down a new file system.

HP Device Access Manager (HPDAM)

HP Device Access Manager speaks to HP's strong commitment to security and its ability to respond to customer needs with innovative solutions. A common assumption with today's PC usage model is that users who are authorized to log on to a personal computer and access sensitive data are also able to copy that information. In reality, this is not always the case. Companies may need to allow users to view sensitive data, but restrict their ability to copy that data. HP Device Access Manager solves that problem. In doing so, it enables a new usage model for personal computing devices.

Through the combination of a Windows service, a custom Filter Driver and Windows ACLs, the device access control policy defined is enforced to "Allow" or "Deny" users and groups' access to devices on the PC.

HPDAM protects against data leaving the PC, either by accident or intentionally (malicious or otherwise), and mitigates against the introduction of malware to the PC.

Accessing Devices

Device Access Manager's true power lies in configuring device access profiles. PC administrators can create device and peripheral usage profiles based on the individual user, user type, individual device, or device class. Configuring device classes or devices will create policies to implement complex security requirements, as well as complex business processes.

Define a policy

Once the administrator authenticates, using the "Change" button, the "Groups on this PC", "Device Classes", "Access" and "Duration" (see "Just In Time Authentication (JITA) Configuration" section) can be modified to create a policy. This level of configurability enables new client policies, as described in the scenarios below:

- Scenario 1 – In a call center environment, call takers have full access to sensitive product and pricing information. The company wants to protect this data and ensure that it is not removed from the premises. This can be accomplished by creating a Device Access Manager policy that prevents removable storage devices such as USB keys and writeable optical drives from being used by unauthorized users.
- Scenario 2 – A company is making sensitive financial information available to an auditor and wants to protect this information from being copied or removed from the notebook. Device Access Manager can allow a policy where this user is denied access to any removable storage devices.

Separate policies can be defined for Administrators and Users. Only Administrators are allowed to change the device access control policy on a machine. Users have a read-only view of the policy that applies to them.

For most device classes, the device access policy is a simple "Allow" or "Deny". The following common device classes within Device Access Manager are supported:

- Removable Storage (any attached storage device that Windows assigns a drive letter to access))
- Optical drives
- Bluetooth
- IEEE 1394 Bus Host Controllers
- Ports (COM & LPT)
- The following are examples of the additional devices supported:
    - Biometric devices
    - Network Adapters
    - Imaging Devices (e.g. Webcam)

Just In Time Authentication (JITA) Configuration

JITA Configuration shown in Figure 5 allows the administrator to view and modify lists of user groups that are allowed to access devices using JITA. JITA-enabled users will be able to access some devices for which policies created in the Device Class Configuration have been restricted.

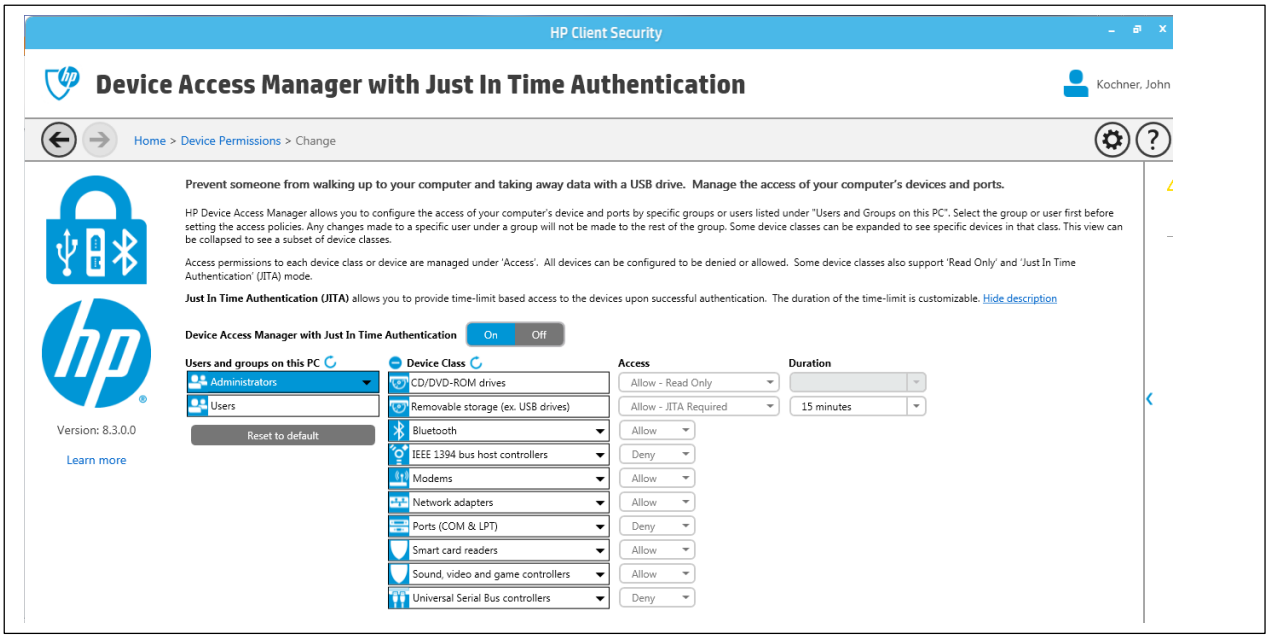

Figure 5 HP Device Access Manager

The JITA period authorization can be for a set number of minutes or an "Unlimited" duration that will not expire. With "Unlimited" duration, users have access to the device from the time they authenticate until the time they log off the system. The JITA period can also be extended one minute before the JITA period is about to expire. The JITA period expires as soon as the user logs off the system or another user logs in ; whether the user is given a limited or unlimited JITA period. The next time the user logs in and attempts to access a JITA-enabled device a prompt to enter credentials displays. Since JITA leverages HP Client Security's Credential Manager, user should be able to authenticate with any applicable/available/enrolled credential as per the session policies.

An example of this is that Device Access Manager can set access to removable storage devices to 15 minutes of access after requiring successful authentication. Once that 15 minute session is over, Device Access Manager will deny access to removable storate without another successful authentication.

JITA is available for Optical drives and Removable Media.

- Along with "Deny", there are 3 "Allow" access configurations.
  - "Allow – Read Only",
  - "Allow – Full Access"
  - "Allow – JITA Required".

Just In Time Authentication will deny access to a device until a user tries to access it. Then, if policy permits, the user can authenticate and gain access to the device for a configurable period of time.

HP File Sanitizer

File Sanitizer allows you to securely shred personal information or files, historical or Web-related data, or other data components on the computer's internal hard drive; and to periodically bleach the computer's internal hard drive.

File sanitization is more intensive process than simple file deletion. When you shred an asset using File Sanitizer, the files are overwritten with meaningless data, making it virtually impossible to retrieve the original asset. A Windows simple delete action may leave the file (or asset) intact on the hard drive or in a state where forensic methods could be used to recover it. The amount of time it takes to delete a file or a group of files is directly related to their size. File Sanitizer is therefore not a replacement for simple file deletion; it is instead meant to complement it.

Bleaching will securely write random data over all free space on the system. This prevents all assets previously deleted, using windows simple deletion, from being recovered

File Sanitizer destroys files by using the US-DOD algorithm which writes 0s first then 1s and then random data which ensures the information in the file cannot be recovered. It does this rewrite three times over the data. It also erases free space using the same rewriting methods.

File Sanitizer cannot be used to sanitize or bleach the following types of drives:

- Solid-State Drives (SSD), including Flash Cache and RAID volumes that span an SSD device
- Solid State Hybrid Drives (SSHD)
- External drives connected by USB, Firewire, or eSATA interface

Shredding

- Shred an individual file/folder or group of files/folders using right click shredding or dropping files on the Desktop Icon.
- Use the Desktop icon to initiate a shred from your scheduled Shred List.
- Schedule a Shred to be performed Once, Daily, Weekly or Monthly.
- Shred Recycle Bin, Temporary System Files, Temporary Internet Files, Cookies, or add Additional Folders.
- Exclude folders from being shredded by adding folders to your Never Shred List.
- Shred on browser close
    - Supported browser: Internet Explorer (IE)

NOTE

Internet Explorer 11 may require a user to disable “Enhanced Protected Mode” in order for File Sanitizer to work.

Bleaching

- Use the Desktop icon to initiate Bleaching process.
- Schedule Bleaching to be performed Once, Daily, Weekly or Monthly

NOTE

It will not be technically possible to apply the same algorithm on SSD, SSHD, or RAID/Flash Cache, etc., Therefore, these drives are considered unsupported.

HP Trust Circles

The HP Trust Circles file and document security application combines folder file encryption with a convenient trusted-circle document-sharing capability. The application encrypts files placed in user-specified folders, protecting them within a Trust Circle. Once protected, the files can be shared with anyone, but only those in the Trust Circle can truly access them. If a protected file is received by a non-member, the file remains encrypted, and the non-member cannot access the contents.

Trust Circles prevents accidental data breach. Having a Trust Circle established between a user and his / her peers allows for near effortless secure data sharing, while also keeping the data at rest protected. No additional passwords required other than your Windows password to authenticate, or using additional credentials as allowed by session policies within HP Client Security.

Data is encrypted at the file level. Depending on the usage scenario, a file is either presented encrypted or decrypted to applications. For example: when attaching a file to an email, the file is presented in encrypted form so the encrypted file will be attached, therefore ensuring protection. Once you have setup Trust Circles for your email you can begin to create Trust Circles. Contacts are invited by email to join a Trust Circle.

There are two ways to send email invitations and to reply to them:

1. Using Microsoft® Outlook - Microsoft Outlook automates the processing of any Trust Circle invitations and responses from other Trust Circle users.
2. Using Gmail, Yahoo, Outlook.com or other email services (SMTP) - when you enter your name, email address, and password; Trust Circles uses your email service to send email invitations to the members selected to join your trust circle.

Trust Circle invitations will include a link that they can click on to download free HP Trust Circles Reader or purchase HP Trust Circles Pro (http://hptc.cryptomill.com).

Once members are confirmed, they will be able to read files you share with them that have been placed in that Trust Circle folder(s). If you should happen to send one of the encrypted files form the Trust Circle to someone that is not a member, they will not be able to read the file.

Technology

- User protected files (Word Docs, PDF's, Excel, etc.) are encrypted using AES 128.
- Internal Trust Circle information (including the Trust Circles encryption keys themselves) are encrypted using AES 256.

Limitations

- HP Trust Circles Standard supports up to 5 Trust Circles each with a maximum of 5 members in each Trust Circle.
- HP Trust Circles Reader, allows you to accept invitations sent out by HP Trust Circles users, and read encrypted files from Trust Circles of which you are a member. It cannot create a Trust Circle.
- HP Trust Circles cannot protect system files or other parts of the operating system such as system folders and the recycle bin.
- Trust Circles is available on select products. Please consult the product's datasheet for more information.

Authentication

- When installed with HP Client Security, authentication is handled through HP Client Security using one of the enrolled authentication methods.
- When installed standalone without HP Client Security, Trust Circles uses your Windows Password for Authentication

- User can change the settings for requiring Periodic Authentication which requires that the user is authenticated after the specified timeout and while performing sensitive operations. This setting allows users the authentication to turn on or off as well as the time limit.

Backup/Restore

- Backups save the internal database and are password protected. This includes the profile, Trust Circles, and member Information; as well as the license information.
- Restore can be done by the user to migrate the Trust Circle settings to a second computer owned by that user.
- The secrets stored in the backup database are protected by the password you created when preforming the backup.

HP Drive Encryption

HP Drive Encryption (HPDE) shown in Figure 6 provides complete data protection by encrypting your computer's data so it becomes unreadable to an unauthorized person. If an encrypted drive is removed from the system and attached to a USB enclosure, it cannot be read from another PC without proper authorization.

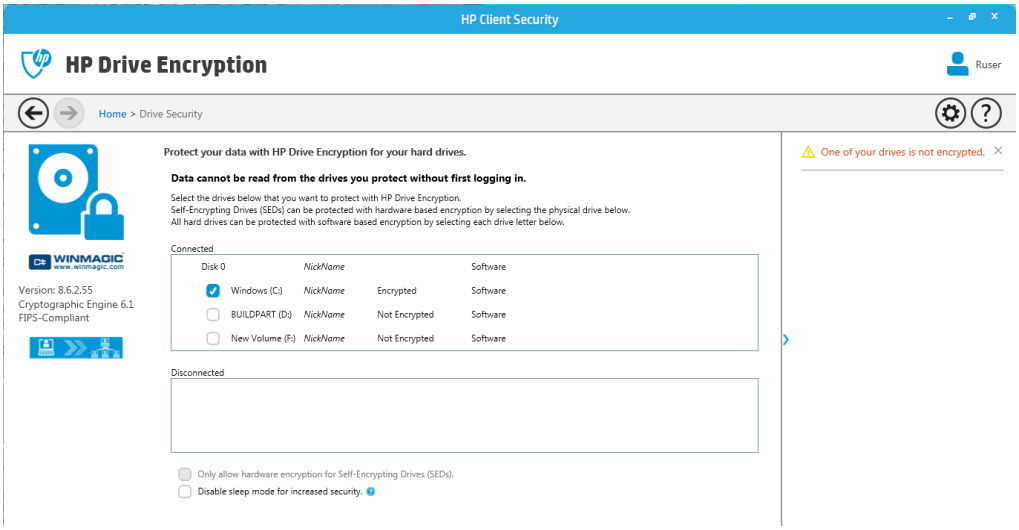

Figure 6 HP Drive Encryption

When the drive is encrypted, the Drive Encryption login window displays before the Windows® operating system starts. Windows requires authentication in the form of a password, smart card or fingerprint before starting.

HP Client Security allows a Windows administrator to perform the following tasks:

- Encrypt or decrypt a partition on an individual hard drive (HDD) or solid state drive (SSD) using software encryption (internal SATA drive and eSATA drive only).
- Encrypt or decrypt OPAL Self Encrypting Drive (SED) using hardware encryption.
- Provide enhanced security by disabling Sleep or Standby to ensure that Drive Encryption pre-boot authentication is always required.
- Create encryption recovery key.
- Recover access to an encrypted computer using encryption recovery key and HP SpareKey.
- Enable Drive Encryption pre-boot authentication using a password, registered fingerprint, or PIN for supported Smart Cards.

Launch via Wizard

HPDE can be activated from HP Client Security Setup wizard shown in Figure 7.

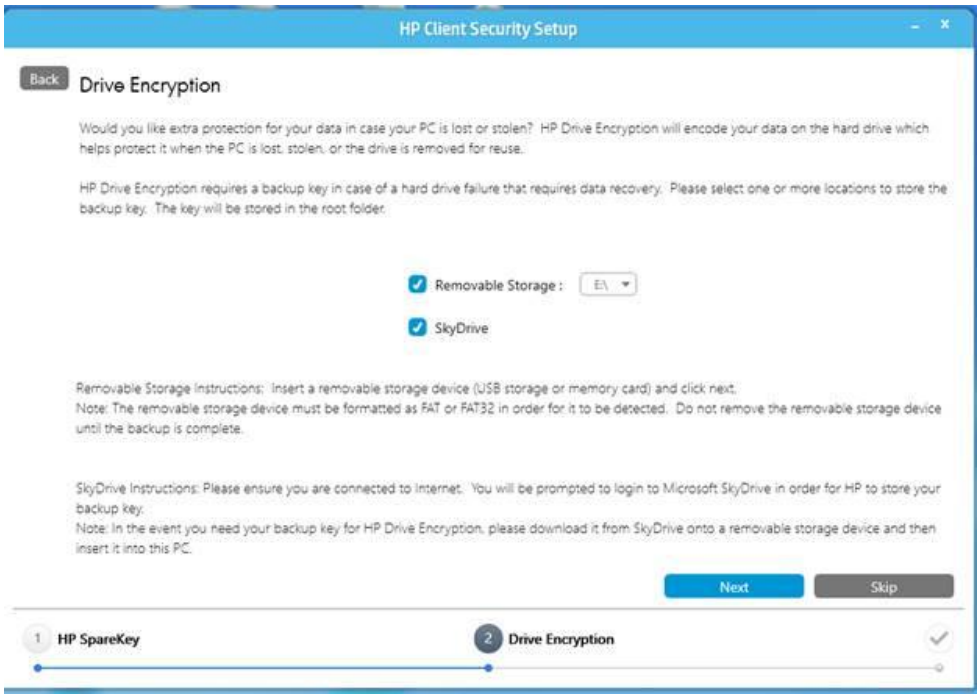

Figure 7 Wizard Page

Completing the wizard performs the following:

- Allows selection of the location for backing up the encryption key. The user can choose either Removable Media or SkyDrive or both. If the encryption key backup fails, an error will be displayed to the user and the wizard will not proceed.
- Activates HPDE:
  - Automatically select and encrypt the primary system partition.
  - Automatically perform hardware encryption - if the primary disk is SED. The whole disk is encrypted except the HP_Tools partition.
  - Use TPM protection for drive encryption on TPM-enabled machines, if TPM is already initialized and owned.
- If you choose not to activate HPDE from the Wizard, you can activate it later via the HP Client Security application.

Launch via HP Client Security

HPDE can be alternatively activated from HP Client Security under "DATA" category shown in Figure 8.

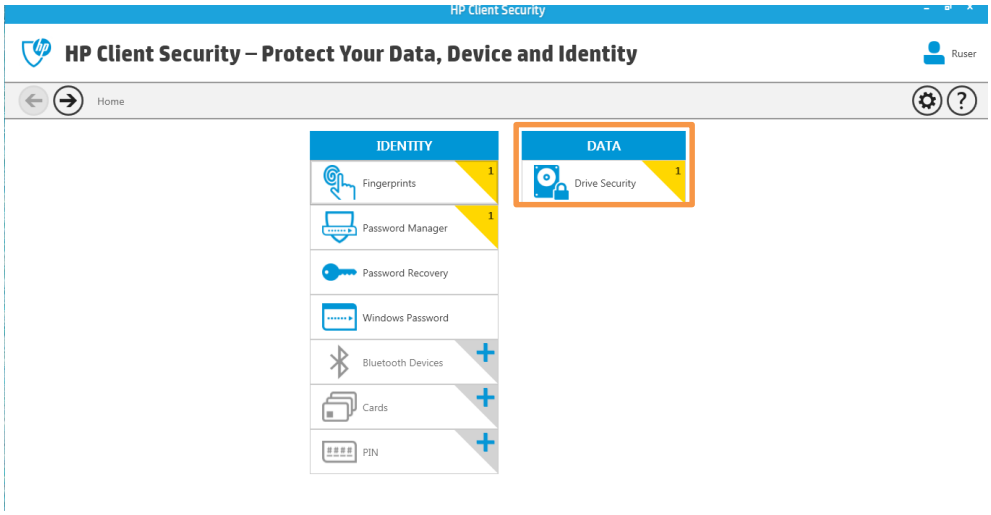

Figure 8 Launch HPDE Using HP Client Security

HP Client Security provides the following options:

- Select partition to encrypt from a list of partitions. The following partitions are not listed:
  - Partition with no drive letter assigned
  - HP_TOOLS
  - HP_RECOVERY
- Select from the following optional features:
  - Disable sleep to enhance security on the system for both software and hardware encryption
  - Enable TPM for enhanced security (available only on TPM-enabled machines)
    - Stores the encryption key in the TPM for enhanced secure storage.
  - Enable software encryption (instead of hardware encryption) on a SED
- Must create encryption recovery key using one or more of the available options:
  - Removable media
  - SkyDrive
  - TPM (available only on TPM-enabled machines; TPM must be owned and initialized)

Notifications

HPDE displays various actionable notifications in two ways as shown in Table 4. Color indicates the severity of the notification and the associated message guides the user to what needs to be done. Notifications can be dismissed by clicking on the 'X' on the right of the notification.

Table 4 Actionable Notifications

Color	Message	Can be dismissed? Yes/No	Action
Red	Your data is at risk. Please encrypt	Yes	• Unless a policy prevents this item

Color	Message	Can be dismissed? Yes/No	Action
	your drive now.		from being dismissed, this can be dismissed. • Upon clicking on the "Requires Attention button", the administrator will be redirected to the HPCS Drive Encryption Activation page.
Yellow 	Your drive is currently being encrypted. When completed, your data will be protected with encryption.	Yes	No action
Yellow 	Your drive is currently being decrypted.	Yes	No action
Yellow 	Your drive is managed. HP Client Security cannot manage this drive.	Yes	Notification appears when the drive is already encrypted and managed by 3rd party software No action
Yellow 	One of your drives is not encrypted.	Yes	• This is only applicable for non-OS partition(s) and/or external drive. • Administrator will be redirected to HPCS Drive Encryption Activation page.
No color	Your data is protected with encryption.	Yes	• If the only drive is the OS partition and if it is encrypted, it will show this notification. • If there is more than one drives (either user created partition and/or external drive attached) and if they are all encrypted, it will show this notification. No action

Technical Details

- Usage
  - Windows Administrator user
    - Can configure HPDE policy.
    - Can activate and de-activate drive encryption.
    - Can backup and restore the encryption key.
  - Windows standard user
    - Cannot configure HPDE policy.
    - Can view the status of the drive. (i.e. if a drive is encrypted or not)
    - Can backup and restore the encryption key.
- Pre-requisites
  - HP Client Security: Version 8.2.x must be installed first
  - 2008 VC ++ version 9.0.30729.6161 Redistributables
  - Microsoft .NET Framework 4.5
- Supported OS's

- Windows 7 (32-bit and 64 bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)

- Supported Languages
  - HPDE supports 35 languages (English, Brazilian Portuguese, Czech, French, German, Italian, Japanese, Korean, Russian, Simplified Chinese, Traditional Chinese (Taiwan/Hong Kong), Spanish, Thai, Arabic, Danish, Dutch, Finnish, Polish, Sweden, Turkish, Bulgarian, Hebrew, Hungarian, Norwegian, Portuguese (Iberian), Slovak, Croatian, Estonian, Greek, Latvian, Lithuanian, Romanian, Serbian, Slovenian).
- Supported SED's (other drives may work, but these have been pre-qualified):

Vendor	Model #	Drive Type	Firmware
Micron	MTFDDAK256MAM-1K12	SSD OPAL	08TH
Seagate Yara	9WU142	OPAL	0001SED7
Samsung (SM 841)	MZ7PD128HAFV-000H7 MZ7PD256HAFV-000H7	SSD OPAL	DXM05H6Q

- Supported Smart Card

Vendor	Model #	Middleware
ActivIdentity	Cyberflex Access 64K V2c	ActivClient7.0.2.25

- Encryption Strength - AES 256
- Certification - FIPS 140-2 Level 1

Pre-boot Authentication

HPDE has it is own pre-boot login environment that requires users to authenticate.

- Windows 8 Native UEFI: When the drive is encrypted, WinMagic's Pre-boot UEFI (PBU) performs pre-boot authentication (PBA) BEFORE the drive can be accessed by the Windows Boot Loader. In order to prevent PBU getting removed from the BootOrder (for example with Windows 8 "Refresh your PC" and Windows 8 "Reset your PC") and thus potentially compromising access to the encrypted disk without authentication, HP and WinMagic implemented the FilterBootOrder (FBO) variable which is created by HPDE pre-boot to register PBA with HP BIOS. HP BIOS is expected to function as designed only if FBO exists. FBO gets removed if HPDE is either uninstalled or if a user performs Windows 8 Reset to Plain Text.
- Windows 7 Legacy: When the drive is encrypted, WinMagic's Pre-boot Linux (PBL) performs pre-boot authentication (PBA) BEFORE the drive can be accessed by the Windows Boot Loader. In order to support F11 Recovery for SEDs, HPDE requires INT15h implementation in HP BIOS. INT15h-implemented HP BIOS will detect if OPAL mode is enabled and then will display F11 Recovery prompt. Without INT15h implementation, HP BIOS cannot determine if the recovery partition is really present or not. When F11 is pressed, HP BIOS stores a value in memory indicating F11 was pressed (to be later returned by an INT15h call) and will then boot the hard drive. This will launch the PBA code which authenticates the user and will launch the recovery partition.
- Authentication and Recovery Methods
  - Authentication: Password, Fingerprint, Smart Card
  - Recovery: SpareKey and recovery using the backed up encryption key

- Drive Encryption pre-boot supports Microsoft SecureBoot if enabled.
- One Step Logon, when configured to work between three domains (BIOS, Drive Encryption and Windows), will bypass Drive Encryption pre-boot after user authenticates at HP BIOS. In the event that Drive Encryption is the first domain to require authentication, One Step Logon will provide authentication to Windows and directly log the user in to the desktop without an additional authentication. This feature may be enabled or disabled by an administrator.

Manageability / Upgradeability to Premium Solutions

WinMagic SecureDoc Enterprise (for HP) is a centrally managed version of the encryption engine included in HPDE that allows HP customers to increase administrative efficiency, improve end user experiences, and reduce the total cost of IT ownership. All while ensuring maximum security and transparency in regular work flow. Easily integrating with industry-standard technologies such as OPAL-compliant SEDs, WinMagic SecureDoc Enterprise (for HP) allows businesses to manage or control the security of their IT environment efficiently.

Should your business require centralized management and control, upgrade seamlessly to WinMagic SecureDoc Enterprise (for HP), even if the drive was encrypted without having to decrypt it first. Ideal for environments with ten devices or more, it can also accommodate tens of thousands of users. Licenses can be transitioned to WinMagic SecureDoc Enterprise (for HP) with minimal impact to end users. Contact your HP Sales representative for additional details. Table 5 provides a comparison of HPDE (preinstalled) and WinMagic SecureDoc Enterprise (for HP).

Table 5 Feature Comparison

Offering	HPDE (Pre-installed)	WinMagic SecureDoc Enterprise (for HP)
Software Full Disk Encryption (FDE/FVE)	✓ (FVE)	✓
Multi-Drive Encryption (external)	✓	✓
RAID Support	✓	✓
Windows 8 refresh/reset support	✓	✓
Onscreen Keyboard for Win 8 Touch	✓	✓
Pre-boot Authentication	✓	✓
One Step Logon	✓ (3 Domains with One Step Logon)	✓ (2 Domain)
Opal SED Support	✓	✓
External Storage Encryption	✓ (via eSata)	✓
Multi-factor Authentication	✓ (HP Client Security)	✓
Key back-up to SkyDrive	✓	✗
Active Directory Integration	✗	✓
Network Pre-Boot Authentication	✗	✓
Wireless Pre-Boot Authentication	✗	✓
Centralized Management Console	✗	✓
Mac OS X support	✗	✓
Linux Support	✗	✓
Intel AT Support	✗	✓

Removable Media Encryption	✗	✓
Removable Media Container Encryption	✗	✓
Dynamic Key Provisioning	✗	✓
File and Folder Encryption	✗	✓

Infineon Trusted Platform Module

HP PC's feature a Trusted Platform Module (TPM) embedded security chip on select HP business notebooks, desktops and workstations. This embedded security chip is certified to the Trusted Computing Group (TCG) Evaluation Assurance Level 4+ (EAL4+) standard. HP platforms support the latest TPM v1.2.

The Trusted Computing Group (TCG) is an international industry standards group. The TCG develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and implementation by the industry. Table 6 provides a list of TPM features and benefits on an HP PC.

TPM Management uses a Microsoft Management Console (MMC) snap-in tool. The TPM Management can be run as a stand-alone console or it can be added/used with MMC.

Table 6 TPM Features and Benefits on HP PC's

Feature	Benefit
Designed to the TCG standard	As a standards-based technology, TPM security chips are designed to work with a growing number of third party software solutions while providing a platform to support future hardware and operating system architectures.
Supports Microsoft CAPI and PKCS#11 cryptographic software interfaces	Enables the TPM security chip to enhance a broad range of existing applications and solutions that take advantage of these interfaces (for example, Microsoft Outlook®, Netscape Navigator, RSA SecurID and public key infrastructure solutions from leaders like Microsoft, VeriSign and Entrust)
Enhanced Microsoft EFS	Helps protect sensitive user data stored locally on a PC, where access to Microsoft EFS encrypted files are protected by the embedded security chip, providing a higher degree of hardware-based protection
Support for TPM v.1.2	HP PC's support the latest TPM v1.2

Some scenarios supported by the embedded TPM module include:

- A computer with the TPM can create encryption keys that can only be decrypted by the same TPM. The TPM "wraps" encryption keys with its own storage root key, which is stored within the TPM. Storing the storage root key in the TPM microchip, rather than on your hard disk, offers better protection against attacks designed to expose your encryption keys. This can benefit multiple security applications that use encryption.
- Also, a TPM owner password is created when TPM is first initialized. The TPM owner password helps ensure that only the authorized owner can access and manage the TPM on the computer.

For more information on trusted computing solutions from HP, including more information on the embedded security chip solution for HP business desktop, notebook and workstation PCs, visit www.hp.com/go/security

OR

Visit: SLB9635 or http://www.infineon.com/cms/en/product/chip-card-and-security-ics/embedded-security/trusted-computing/trusted-platform-module-tpm1.2-pc/channel.html?channel=ff80808112ab681d0112ab6921ae011f.

HP Computrace and HP Absolute Data Protect

HP Computrace provides a single cloud-based console (http://cc.absolute.com) for administrators and users who want to persistently track and secure all of their endpoints. Computers can be remotely managed and secured to ensure - and most importantly prove - that endpoint IT compliance processes are properly implemented and enforced.

With select Absolute products you can:

- Locate a missing PC
- Remotely delete data
- Remotely lock a PC
- Recover a stolen PC

Additional products offered by Absolute Software are: Computrace Complete, Computrace Data Protect, Computrace Mobile and Computrace One.

Computrace provides foundational support for all activities related to Governance, Risk Management, and Compliance (GRC) for the endpoint. By maintaining a persistent connection to each device, organizations can take advantage of or oversee:

- Data Security & Protection
- Deployment & Licensing Audits
- BYOD policy enforcement
- Theft Recovery
- Theft and criminal investigations
- Endpoint forensics
- Security incident response & remediation
- Compliance reports & certificates
- Asset Administration
- Geotechnology (Geolocation/Geofencing)

Since most HP devices have a BIOS Absolute Persistence module, the service will continue to function once activated even if the software is uninstalled or the hard drive is reimaged. The Computrace Agent is backwards compatible and provides support back as far as Windows NT.

As of 2013, Absolute has recovered more than 30,000 devices in more than 100 countries.

Visit http://www.absolute.com/en/landing/partners/13/hp via the “Learn More” link on the HP Client Security Computrace module page.

For a complete listing of HP BIOS models, visit: http://www.absolute.com/en/partners/oem/hp

For further questions on upgrading, contact: hp@absolute.com.

Absolute Data Protect (ADP)

Absolute Data Protect from Absolute Software enables individual users to:

- Remotely Locate your device
- Remotely Lock it to prevent unauthorized access

- Remotely Delete personal data in the event of theft or loss

HP ElitePad 900 G1 and EliteBook Revolve 810 with Windows 8.x include a 4 year license of Absolute Data Protect.

All devices with ADP also feature the BIOS Absolute Persistence module. If the Agent is removed or missing, the persistence module will automatically reinstall itself so you can stay connected with your device even when it's lost or stolen.

On devices that include Absolute Data Protect (ADP) out of the factory, an Absolute Reminder application allows the user to install and activate ADP via an icon or Windows 8 start menu tile. In addition, HP Client Security alerts the user accordingly.

If activated but the device has not called home in a certain number of days, ADP sends an alert to the ADP module page A yellow alert for 3 to 7 days or red for more than 7 days. The users are prompted to request an immediate agent call or given a link to the Consumer Customer Center login page at https://my.absolute.com/.

Individual Customers can choose to upgrade to LoJack for Laptops Premium which provides additional theft recovery and a service guarantee - more information can be found at http://www3.absolute.com/lojackforlaptops .

How It Works

ADP installs a stealthy and persistent agent on each device. The agent has no dependencies on Windows Presentation Foundation (WPF) or .NET. The agent calls home frequently to report on its status and to check for any server initiated actions such as data delete, device freeze, the filing of a theft report, or other endpoint actions. IT Administrators can remotely report on and manage all devices from a central management console ("Commercial Customer Center"). The patented Absolute persistence technology ensures that the agent software is always present and running so that the device stays connected.

Communication between the Agent and the Monitoring Center uses:

- Key delivery RSA 1024, session encryption - GCM with AES 128 Optional
- FIPS encryption 140–2: Key delivery RSA 3072, session encryption GCM with AES 128

Appendix A - Frequently Asked Questions

Q. What authentication technologies are supported by HP Client Security?

A. HP Client Security Manager is a security platform that has been designed to easily grow with the user's needs. It supports the following authentication technologies currently, but may support additional technologies as they become available.

- Password
- Fingerprint
- Smart Card, Contactless Card, Proximity Card
- Bluetooth
- PIN

Q. How does Smart Card security compare to fingerprint security?

A. HP Client Security supports both Smart Card authentication and fingerprint authentication. Since both devices store secrets using hardware protection, they have similar levels of security. Smart cards may be a better fit for large organizations with the infrastructure to support creation and enrollment of certificates. Smaller organizations may prefer the convenience of fingerprint authentication.

HP business notebooks offer both integrated Smart Card readers as well as integrated fingerprint reader sensors. HP's fingerprint sensors provide higher security than many external fingerprint scanners. This higher security includes an on-sensor credential vault and on-sensor match before credential release. Smart cards store credentials on the card and use a PIN to release the credentials.

NOTE

A very high level of security can be achieved by requiring both Smart Card AND fingerprint authentication for access to critical assets.

Q. Is there a cost associated with HP Client Security?

A. HP Client Security and security modules are available as standard security features on most business notebooks. On business desktops or workstations, some modules are available at additional cost.

Q. Can Smart Cards be used for pre-boot authentication?

A. Smart cards are not supported in BIOS. However, Drive Encryption login has select Smart Card support.

Q. How can I tell if my PC contains a TPM embedded security chip?

In general, if the PC contains a TPM embedded security chip, it will be listed in the Windows Device Manager, under the category *Security Devices*. On business PC's, the TPM embedded security chip will be listed as *Infineon Trusted Platform Module*. However, TPM may be hidden/disabled in BIOS.

Q. Regarding the TPM chip itself, does it store any user specific information? If so, how can I clear it?

A. No. The TPM can be cleared via F10 Computer Setup Menu to return to factory default/cleared state.

Q. How does Credential Manager differ from other single sign-on solutions?

A. Most technologies and features provided by HP Client Security Manager are individually available. The value of HP Client Security is that it brings these technologies together in a single, easy to use security solution. As an HP Client Security core component, the features provided by Credential Manager are integrated into HP Client Security and work with the user authentication features of HP Client Security. Additionally, 2-factor authentication can be enforced depending on what level of security is required. Additionally, authentication in the pre-boot environment only supports a single factor, however the user must still provide both factors before logging into Windows.

Q. Does Credential Manager for HP Client Security use the embedded TPM security chip if available?

A. Yes, Credential Manager uses the embedded security chip, if available and owned, to encrypt passwords stored in the password vault.

Q. Does Credential Manager for HP Client Security support multiple users on a single client device?

A. Yes.

Q. What if a user has multiple Microsoft Windows accounts on the same PC? Can Credential Manager still be used?

A. Yes, this would function the same as multiple users on a single PC. The user must use different fingers with each account if they would like to login using their fingerprints. Fingerprint sensor will not accept a finger that is currently enrolled.

Q. What is the difference between user and administrator rights for Credential Manager for HP Client Security?

A. An administrator has full rights to all Credential Manager configuration options. A (limited) user can use the Credential Manager for authentication and the One Step Logon features, but does not have access to the Authentication and Credential configurations, policies, or the Advanced Settings.

Q. If multiple PCs are used by the same user, can the user migrate all of their credentials to the different PCs?

A. No. However, Password Manager data can be backed up to be then restored on another PC in order to transfer all of the application and website usernames and passwords.

Q. Is Credential Manager supported on non-HP computers?

A. No.

Q. Is the HP Client Security software suite available on a non-Microsoft Windows environment?

A. No.

Q. What type of smart card is needed for HP Client Security?

A.

- Windows: All PKI Smart Cards supported via a PKCS11 or CSP stack.
- BIOS: None
- Drive Encryption: ActivIdentity Cyberflex Access 64K V2c,

Q. What is the process for uninstalling HP Client Security?

A. HP Client Security application and the associated software applications can be removed using the Windows Uninstall Program utility in the Windows Control Panel. The process is the same as uninstalling any Windows application. Uninstall all HP Client Security associated software applications before uninstalling the HP Client Security application.

Q. Is Disk Sanitizer available as a product, available standalone or only as part of HP Client Security? Where is the information about the hardware it might or might not work on?

A. HP Disk Sanitizer is a feature built into most HP Business Notebook's BIOS, 2006 and later. HP Disk Sanitizer External edition is available on hp.com for supported HP Business Desktops. Supports traditional hard drives only.

Appendix B- Certifications and Standards

- HP Drive Wncryption
  - WinMagic Cryptographic Engine 6.1 is FIPS 140-2 Level 1 certified (for HP Business PCs introduced in 2013)
  - McAfee encryption engine is not FIPS 140-2 certified (for HP Business PCs introduced prior to 2013)
- **Fingerprint Readers (Integrated on notebooks)**
  - NIST Compliant: No
  - Not FIPS 201 compliant
  - Even though the HP Fingerprint Reader is very secure, it does not support FIPS 201 mainly because FIPS 201 requires a touch sensor instead of a swipe senor.
- **Fingerprint Readers (Integrated on ElitePad Security Jacket)**
  - FIPS 201 certified
- **Smart Card Support**
  - PKI Smart Cards supported via a PKCS11 or CSP stack – with HP Smart Card Keybards and integrated Smart Card readers - FIPS 201 certified
  - Support PC Smart Card industry standard – PC/SC 2.0
  - Support ISO7816 Class A, B and C (5V/3V/1.8V) card
  - Supported: HID iCLASS and Proximity; MiFare Classic 1K, 4K, and Mini - with OMNIKEY 5321 and 5325 readers
- **TPM (Common Criteria Certified TPM)**
  - Advanced Crypto Engine (ACE) with RSA support up to 2048 bit key length
  - Hardware accelerator for SHA-1 hash algorithm 160-bit
  - Infineon's TPM 1.2 is Common Criteria certified at Evaluation Assurance Level (EAL) 4+ Moderate
  - TSS software stack compliant to TCG specifications
  - TPM Cryptographic Service provider (CSP)
- FIPS Link to Wikipedia (General Definition Article)

FIPS_140 or http://en.wikipedia.org/wiki/FIPS_140