HP ProtectTools Security Manager

Introduction

As computers are getting increasingly mobile and better connected, threats to data security are increasing in magnitude as well as complexity. Correspondingly business customers, for whom data security can have a direct impact on the health of their business, are becoming increasingly concerned about this problem.

HP saw the need for a better security solution very early, and started devoting resources to solving this problem. Knowing that security needed to be addressed holistically, HP required the solution to bring many technology areas together in a way that helps ensure not only protection for client devices, but also helps ensure that client devices themselves do not become points of vulnerability that could be used to threaten the entire IT infrastructure.

As a result of this proactive effort, HP has developed a solution, the HP ProtectTools Security Manager, that not only meets the above requirements, but is also extensible and therefore can easily grow to handle new threats and offer new technologies as they become available.

The security dilemma

Businesses trying to implement client device security face a dizzying number of choices that may not always work well together. In addition, security solutions can be difficult to deploy and use. If a technology is difficult to use, most users will avoid using it, and this further complicates the task of making client devices secure.

Client device security options feature a number of capabilities based on a variety of technologies:

- Notebook and desktop computers can be configured with Smart Card readers
- The Trusted Platform Module , or TPM embedded security chip designed to the Trusted Computing Group (TCG) standard, is available on a range of HP products
- Biometrics and RFID (Radio Frequency Identification) are expected to become more important as those technologies mature and become more suitable for enterprise deployment

In addition, many client devices include security features that exist within the device BIOS. These include features such as:

- Pre-boot authentication – ability to authenticate a user before allowing the system to boot
- Device configuration lock down
- Remote management capabilities

While these security features increasingly rely on established industry standards, and therefore better integrate with other elements of IT security, there are still challenges that are keeping these features from being widely deployed and used. These challenges include:

- Usability: technologies and features that are difficult to use
- Manageability: technologies and features that are difficult to manage, particularly on a large scale
- Awareness: IT managers and users are not aware of a feature, or do not understand its purpose
- Interoperability: features or services that span multiple technologies
- Extensibility: solutions that adapt as security needs grow and newer technologies and features become available

The HP ProtectTools Security Manager is a security platform that addresses these challenges by using add-on software modules, which provide important client security features. New features can easily be added by installing new modules. This architecture gives users an easy to use all in one security solution.

HP ProtectTools Security Manager

At the heart of the security strategy for business notebooks, desktops and workstations is the HP ProtectTools Security Manager – this single client console application unifies security capabilities of HP client PCs under a common architecture and single user interface. Today, a range of features is being delivered that build on underlying hardware security building blocks such as TPM embedded security chips designed to the Trusted Computing Group (TCG) standard and Smart Card technology. Collectively these features are addressing business customer needs for better protection against unauthorized PC access, as well as stronger protection for sensitive data stored locally or accessed over a network.

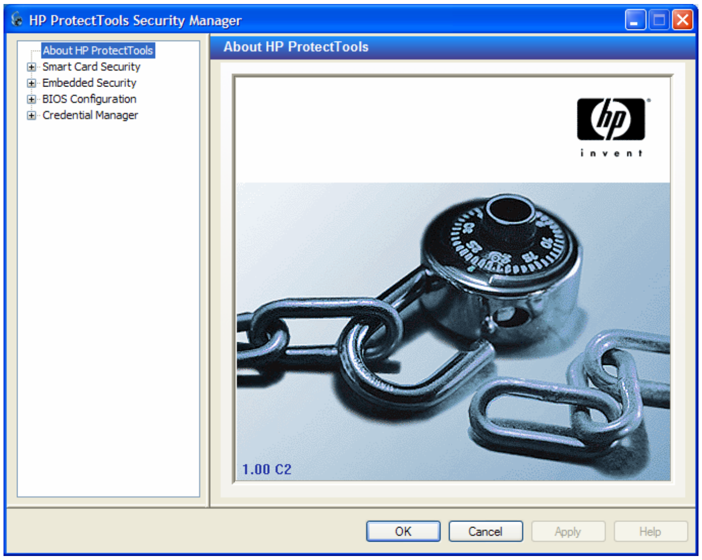


Figure 1 - HP ProtectTools Security Manager Console

HP ProtectTools Security Manager embodies an extensible framework that is designed to allow security software functionality to be added through add-on modules. This approach supports longer term client device security strategy by enabling HP to introduce new functionality over time, but in a highly integrated manner. Ultimately, customers benefit from security features that are easier to use, manage, and provide enhanced value through features that play off of multiple security hardware attributes of the client device.

HP ProtectTools Security Manager is only the first step. The application is a security platform that gets it's functionality via plug in software modules. A number of software modules are also being introduced that provide better protection against unauthorized access to the PC, while making access to the PC and network resources simple and convenient for authorized users.

Features include support for broad multifactor user authentication where a number of different security technologies, such as Smart Cards, biometric fingerprint readers or TPM embedded security chips, can be used to authenticate users. Users are provided with more secure as well as convenient alternatives to passwords when logging into a Microsoft Windows PC. HP is also extending the HP ProtectTools Security Manager feature set to include a client-centric single sign-on capability that conveniently stores and protects many of the credentials users need daily to access websites, network resources and applications.

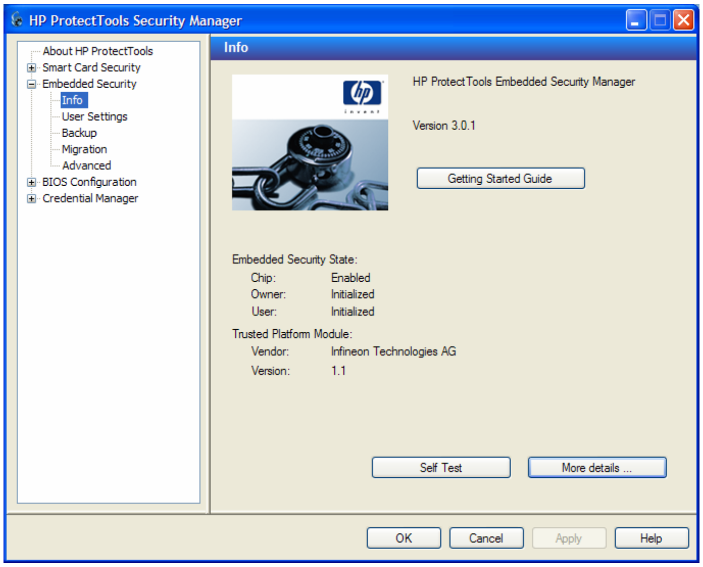
Additional modules are also available that deliver a higher degree of client device security from the moment power is turned on. By leveraging underlying security technologies such as a TPM embedded security chip, HP is enabling better protection against unauthorized access even prior to allowing the operating system to load.

Security Software Modules for HP ProtectTools

This section provides more details on specific add-on security software modules available for use with the HP ProtectTools Security Manager. The modular architecture of the HP ProtectTools Security Manger enables add-on modules to be selectively installed by the end user or IT administrator, providing a high degree of flexibility to customize HP ProtectTools depending on security needs and the underlying hardware configuration. Several of the add-on modules are adapted versions of previously released stand-alone security applications. Integrated into the HP ProtectTools platform, they form a holistic security solution. Going forward HP expects to continue to expand its client security offerings with additional modules for the HP ProtectTools Security Manager.

Embedded Security for HP ProtectTools[1]

Embedded Security for HP ProtectTools is an add-on module for the HP ProtectTools security manager that allows users to configure how they would like to use the TPM embedded security chip. This add-on module is intended for client devices configured with a TPM embedded security chip designed to the Trusted Computing Group (TCG) standard.



HP ProtectTools Embedded Security Manager

Version 3.0.1

Embedded Security State:

Chip:	Enabled
Owner:	Initialized
User:	Initialized

Trusted Platform Module:

Vendor:	Infineon Technologies AG
Version:	1.1

Figure 2 - Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools provides important client security functionality where a TPM embedded security chip is used to help protect against unauthorized access to sensitive user data or credentials. Features accessed through Embedded Security for HP ProtectTools include:

- Administrative functions such as taking ownership and managing the owner pass phrase
- User functions such as user enrollment and managing user pass phrases
- Feature configuration including setting up enhanced Microsoft EFS and Personal Secure Drive for helping to protect user data management functions such as backing up and restoring the key hierarchy as well as key migration

Embedded Security for HP ProtectTools is supported on all HP business notebooks, desktops and workstations that can be configured with a TPM embedded security chip option.

[1] Support for the TPM embedded security chip was previously provided as part of a standalone application called HP ProtectTools Embedded Security Manager. Beginning in early 2004, all subsequent support for the TPM embedded security chip will be delivered through the Embedded Security for HP ProtectTools module and will require the HP ProtectTools Security Manager application.

Table 1 – Embedded Security for HP ProtectTools Features and Benefits

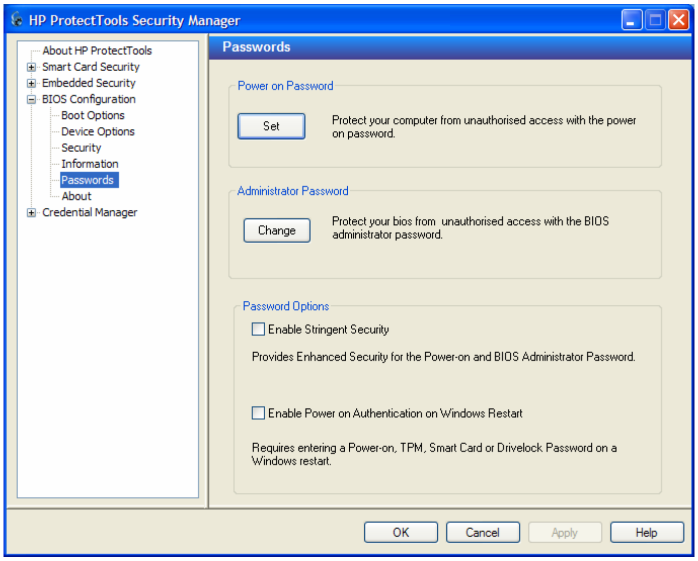
Feature	Benefit
Works with HP ProtectTools Security Manager	User interface is fully integrated into the HP ProtectTools Security Manager. Increases the functionality of the entire security solution by allowing access to the TPM embedded security chip. For example, if the TPM embedded security chip is present, Credential Manager for HP ProtectTools uses it to further secure the encryption keys that encrypt sensitive user credentials such as website passwords or network logon credentials.
Designed to the Trusted Computing Group (TCG) standard	As a standard based technology, TPM embedded 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 embedded 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 infrastructures solutions from leaders like Microsoft, Verisign and Entrust.)
Enhanced Microsoft EFS and Personal Secure Drive (PSD) features encrypt user data	Helps protect sensitive user data stored locally on a PC, where access to the encryption is protected by the TPM embedded security chip providing a higher degree of hardware-based protection.

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

BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools provides access to the BIOS security and configuration settings from within the HP ProtectTools Security Manager application. This feature provides authorized users with a convenient way to access system security features that are managed by the system BIOS.

With BIOS Configuration for HP ProtectTools, authorized users can get access to power-on user and administrator password management, and they can configure pre-boot authentication features, such as Smart Card, power-on password and the TPM embedded security chip.



Power on Password

Set — Protect your computer from unauthorised access with the power on password.

Administrator Password

Change — Protect your bios from unauthorised access with the BIOS administrator password.

Password Options

☐ Enable Stringent Security

Provides Enhanced Security for the Power-on and BIOS Administrator Password.

☐ Enable Power on Authentication on Windows Restart

Requires entering a Power-on, TPM, Smart Card or Drivelock Password on a Windows restart.

Figure 3 – BIOS configuration for HP ProtectTools

With BIOS Configuration for HP ProtectTools, authorized users can:

- Manage power-on user and administrator passwords
- Configure pre-boot authentication features such as Smart Cards, Power-on Passwords, and Drivelock
- Enable/Disable hardware features such as CD-ROM boot.
- Configuring boot options including disabling the ability to boot to drives other than the primary hard drive

Table 2 - BIOS Configuration for HP ProtectTools Features and Benefits

Feature	Benefit
Works with HP ProtectTools Security Manager	User interface is fully integrated into the HP ProtectTools Security Manager.
Provides access to BIOS security and configuration features from within the operating system	Provides an easier to use alternative to the pre-boot BIOS configuration utility known as F10 Setup.
Enhanced security feature set that take advantage of other HP ProtectTools supported security technologies such as Smart Cards and TPM embedded security chips	Provides better protection against unauthorized access to the PC through features that help protect the system from the moment power is turned on. TPM embedded security chip pre-boot authentication requires that users securely authenticate to the chip prior to allowing the system to boot, which helps protect against attacks that exploit the ability to boot to alternative operating system environments. TPM embedded security chip enhanced Drivelock protects a hard drive from unauthorized access even if removed from a system without requiring the user to remember any additional passwords beyond the TPM embedded security chip user pass phrase. Working with Smart Card Security for HP ProtectTools, pre-boot Smart Card authentication requires users to present their Smart Card prior to allowing the system to boot.

Enabling access to BIOS security configuration from within the HP ProtectTools Security Manager creates an integrated security solution and enables authorized users to control every aspect of security management from a single application with a common user interface. The following table describes the key BIOS security features[2] that become accessible from the HP ProtectTools Security Manager using the BIOS Configuration Module.

Table 3 **- Key BIOS security features made accessible by the BIOS Configuration Module**

Feature	Description	Benefit
TPM embedded security chip pre-boot authentication	Utilizes the TPM embedded security chip for user authentication. Users need to input the basic user key pass phrase	Helps protects against unauthorized access to the PC by preventing access to the computer by booting from a device other than the primary hard drive. Provides security benefits similar to a power-on password; however, by allowing the user to use their TPM embedded security chip pass phrase, users are not required to remember an additional password.
TPM embedded security chip enhanced Drivelock	Requires a user to authenticate to the TPM embedded security chip before a Drivelock protected hard drive can be accessed. A separate Drivelock password is not required.	Drivelock helps protect a hard drive from unauthorized access even if physically removed from a system. Allows very strong, random Drivelock passwords to be automatically set in a way that is completely transparent to users (does not require the user to remember another password) Ties a hard drive to a specific system with a specific TPM embedded security chip, preventing other systems from accessing the hard drive if it is physically removed from the original system.

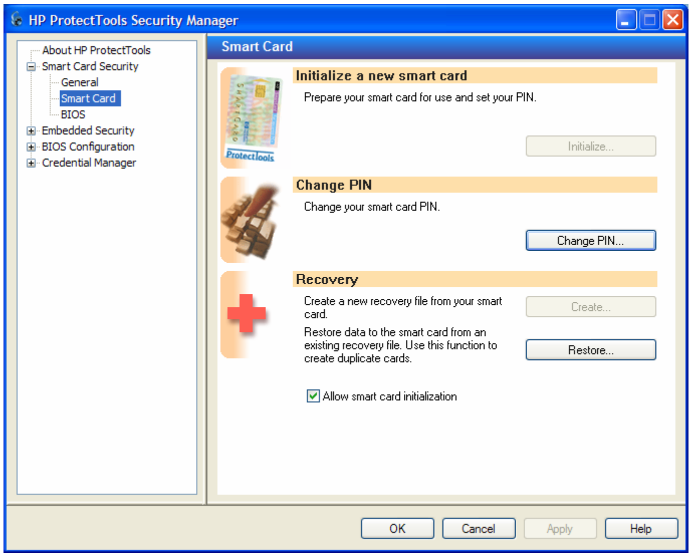
[2] Pre-boot authentication features are available on select platforms. Refer to platform specific specifications for more details.

Feature	Description	Benefit
Smart Card pre-boot authentication	Requires a user to insert a Smart Card and, optionally, enter a PIN to authenticate prior to an operating system being allowed to load	Protects a system from unauthorized access by requiring a user to insert their Smart Card to boot the system. The same Smart Card used to authenticate a user in the pre-boot environment can also be used with HP ProtectTools to login into Microsoft Windows XP or Windows 2000.

BIOS Configuration for HP ProtectTools is supported on most HP business notebooks, desktops and workstations. Enhanced authentication features are supported on select business PCs including the nc and nw series notebooks as well as the dc7100 desktop PC series.

Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools enables access to Smart Card configuration and security features on systems equipped with a Smart Card reader. Smart Card readers can either be integrated, or can be added using the PC card slot. For authentication, users require a Smart Card such as the HP ProtectTools Smart Card[3] which can hold their passwords and PIN, and a supported reader, such as the HP PC Card Smart Card Reader.



Initialize a new smart card

Prepare your smart card for use and set your PIN.

Change PIN

Change your smart card PIN.

Recovery

Create a new recovery file from your smart card.

Restore data to the smart card from an existing recovery file. Use this function to create duplicate cards.

☑ Allow smart card initialization

Figure 4 - Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools provides Smart Card management features such as:

- Initialize and configure an HP ProtectTools Smart Card, which enables a Smart Card to be used for user authentication
- Interface with the BIOS to enable/disable Smart Card pre-boot authentication
- Configure separate Smart Cards for administrators and users
- Set and change the Smart Card PIN
- Backup and restore credentials stored on the Smart Card

Smart Card support was previously provided as a standalone application called HP ProtectTools Smart Card Security Manager. All subsequent Smart Card support will be delivered through the Smart Card Security for HP ProtectTools module and will require the HP ProtectTools Security Manager application. The new module brings a previously separate security technology into the new integrated security solution, giving users a single application from which to manage all security features.

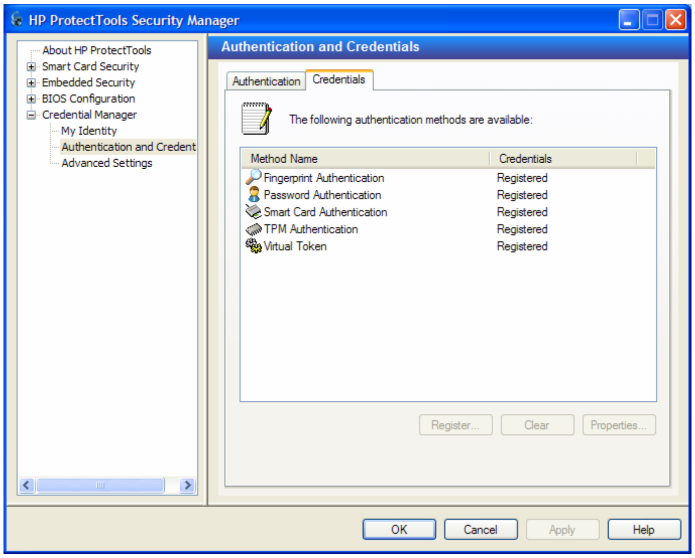
[3] The HP ProtectTools Smart Card part number is DR032A.

Table 4 - Smart Card Security for HP ProtectTools Features and Benefits

Feature	Benefit
Initialize and configure Smart Card security features such as pre-boot Smart Card authentication.	Provides a complete Smart Card security solution for pre-boot and Windows user authentication providing enhanced protection against unauthorized of the PC.
Backup and restore credentials stored on a user's Smart Card.	Provides a mechanism to recover from a situation where a user or administrator loses their Smart Card.
Provides the ability to configure an administrator Smart Card that can be used on multiple systems to access BIOS configuration settings.	Allows an administrator to configure a single Smart Card (or multiple cards) that can be used to securely access BIOS configuration settings without requiring the use of a BIOS administrator password.

Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools is the glue that brings the different security technologies together to create a behavior. Credential Manager gives users the ability to specify how the different available security technologies work together to provide protection against unauthorized access to the client.



The following authentication methods are available:

Method Name	Credentials
Fingerprint Authentication	Registered
Password Authentication	Registered
Smart Card Authentication	Registered
TPM Authentication	Registered
Virtual Token	Registered

Figure 4 – Credential Manager for HP ProtectTools

These technologies include Smart Cards, Biometrics, USB Tokens and other future technologies. Through the Credential Manager, users can create a unique security behavior that requires their chosen authentication method, including alternatives to passwords when logging on to Microsoft Windows. Credential Manager also provides a single sign-on capability that automatically remembers credentials for websites, applications, and protected network resources. Credential Manager effectively is a personal password vault that makes accessing protected information more secure and convenient.

Key features of Credential Manager include:

- Fully integrated with HP ProtectTools Security Manager
- Support for Smart Cards, Biometric fingerprint security, USB Tokens, Virtual Tokens and Passwords
- Single sign-on capability protects passwords for websites, applications and network resources

Table 5 **- Credential Manager for HP ProtectTools Features and Benefits**

Feature	Benefit
Multifactor authentication support	Brings together the available (integrated and add on) security technologies on a PC into a cohesive and unique behavior that utilizes these technologies to authenticate users based on user preferences.
Windows logon capability	Enables the use of any supported security technology to logon onto Windows providing a more secure and convenient alternative to password authentication.
Single sign-on manages user credentials for websites, applications and protected network resources	Users no longer need to remember multiple passwords for protected websites, applications and network resources. Single sign-on works with multifactor authentication capabilities to add additional protection requiring users to re-authenticate when accessing particularly sensitive data. Registering new websites, applications or network logon dialogues is fully automated making it easy for users to begin taking advantage of the added convenience and security of the single sign-on feature.

Platform Support

HP ProtectTools Security Manager is supported across a range of HP business notebooks, desktops and workstations. Please check the product specifications for availability.

Frequently Asked Questions

Q. What add-on modules are currently available for HP ProtectTools Security Manager?

A. Currently the following four modules are available. More modules will be developed and released in the future.

- Smart Card Security for HP ProtectTools
- BIOS configuration for HP ProtectTools
- Embedded Security for HP ProtectTools
- Credential Manager for HP ProtectTools

Q. What authentication technologies are supported by HP ProtectTools

A. HP ProtectTools 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 can easily support additional technologies as they become available.

- Smart Card authentication
- Biometric (Fingerprint) authentication
- USB Token
- Virtual Token
- Password authentication

Q. How does the Smart Card security solution compare to the Biometric solution. Why did HP select Smart Card security over biometric security?

A. Biometric security has long term potential; however, biometric security is not yet fully suited for enterprise deployment because of a lack of enterprise grade features such as support for PKI encryption. Biometric security technology is also considerably higher cost compared to Smart Card technology and because of that, while biometrics attracts a lot of attention, enterprise customers are not ready for actual deployment.

Q. Which HP platforms support HP ProtectTools and the different add-on modules?

A. Please refer to the "Platform Support" section of this white paper.

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

A. Yes, Smart Cards can be used for pre-boot authentication. Please refer to the user documentation that came with your computer for steps to configure the system for Smart Card pre-boot authentication.

Q. Do HP clients support large scale deployment of the TPM embedded security chip?

A. Embedded Security for HP ProtectTools includes a number of configuration settings that can be managed through a Windows security policy template. Refer to the technical White Paper on embedded security published online (ftp://ftp.compaq.com/pub/products/security/embedded_security_-_implementation.pdf). Additional information can also be found in the Embedded Security for HP ProtectTools online help files.

There are also third party software solutions that can help with managing TPM embedded security chips on a large scale. Wave Systems has a solution that enables security chip key management and roaming. Infineon Technologies is another important HP partner in security. We have collaborated extensively on our Embedded Security and Credential Manager for HP ProtectTools modules. As part of Infineon's broader portfolio of security capabilities they are in the final stages of developing a back-end security management solution that works with HP ProtectTools. It addresses TPM embedded security chip key management and provides highly manageable enterprise single sign-on capability when used with Credential Manager for HP ProtectTools.

HP business PCs and business notebooks will also support large scale deployment of TPM embedded security chips by allowing certain one time configuration processes to be scripted. This script support is available today on business desktops today. Business notebooks that feature a TPM embedded security chip require a BIOS update that is expected to be made available by the end of 4Q04. HP has documented this support through a white paper and sample script that can be made available to customers upon request (refer to Softpaq 27958).

Q.What are HP's internal security policies?

A. HP IT is in the process of rolling out a new USB Security Token to be used for strong multifactor authentication when accessing the corporate network over VPN. Credential Manager for HP ProtectTools has been designed to support this token enabling it to be used not only for VPN access, but when logging into Windows with Credential Manager or as additional protection for the Credential Manager single sign-on service.

Q. What is the Credential Manager module for HP ProtectTools?

A. Please refer to the "Credential Manager for HP ProtectTools" section of the white paper.

Q. How does Credential Manager differ from other Single Sign On solutions?

A. Most technologies and features provided by HP ProtectTools security manager are individually available. The value of HP ProtectTools is that it brings these technologies together into a single easy to use security solution. As an HP ProtectTools add-on, the features provided by Credential Manager are integrated into HP ProtectTools and work with the user authentication features of HP ProtectTools.

Q. Does Credential Manager for HP ProtectTools utilize the TPM embedded security chip if available?

A. Yes, Credential Manager uses the TPM embedded security chip, if available, to encrypt passwords stored in the password Vault.

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

A. Yes, Credential Manager works on the concept of "Identity". In order to log on to a computer, a user simply needs to create a Credential Manager ID.

Q. What if a user has multiple windows accounts?

A. This would function the same as multiple users on a single PC. The user would have to create a different Identity for each account.

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

A. An administrator has full rights to all Credential Manager Configuration options. A user can use the credential manager for authentication and use the single sign-on features, but does not have access to the Authentication and Credential configuration or the Advanced Settings.

Q. What if a user utilizes multiple PCs, can the user's identity be used on different machines?

A. No, however a user's credential can be copied in order to be used on another PC.

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

A. Credential Manager for HP ProtectTools requires HP ProtectTools to be present on the system. If the client device is running HP ProtectTools, it will support Credential Manager.

Q. Can Windows logon via Smart Card or other security devices available without Credential Manager for HP ProtectTools?

A. No, Credential Manager for HP ProtectTools is required for Windows Logon with a Smart Card or other security device.

Additional Resources

1. *HP ProtectTools Embedded Security – the HP Trusted Computing Implementation*, Hewlett-Packard Company, October 2003.
2. *HP Embedded Security for ProtectTools - Embedded Security Chip Pre-Boot User Authentication*, Hewlett-Packard Company, January 2005.
3. *HP ProtectTools Embedded Security – Expanding Trust Within the Enterprise Computing Environment*, Hewlett-Packard Company, May 2003.
4. *ProtectTools Smart Card Security Manager*, Hewlett-Packard Company, July 2003.
5. Pearson, Siani, et al, *Trusted Computing Platforms: TCPA Technology in Context*, Prentice Hall PTR, July 2002.

5982-9847EN, 11/2004