



WW PSG Sales and Marketing

May 2003

white paper

# hp ProtectTools Embedded Security - expanding trust within the enterprise computing environment

## contents

- introduction..... 3**
- security ..... 3**
- conventional security solutions..... 4**
- trusted computing standards..... 5**
  - Trusted Computing Group..... 5
- hp ProtectTools Embedded Security ..... 5**
  - overview ..... 6
  - ProtectTools Embedded Security ..... 6
  - PC implementation ..... 7
  - extending trust – throughout the platform ..... 7
  - extending trust – to the network ..... 8
- sample scenarios..... 10**
- summary..... 13**
- for more information ..... 14**
- appendix a – HP security solutions ..... 15**
  - ProtectTools ..... 15

**abstract:** ProtectTools Embedded Security technology from HP allows the customer to establish a trusted computing environment, helping to answer the following questions: Can I trust this platform to operate safely on my network? Is the platform configured appropriately? Is sensitive information on this platform protected?

For computer owners, a trusted computing environment protects information assets and makes computing devices more manageable, reducing total cost of ownership. For businesses, trusted computing protects e-transactions, helps to reduce liability and enables e-business growth, creating a competitive advantage. For OEMs, trusted computing provides product differentiation and builds brand trust.

Through its leadership position in the Trusted Computing Group (TCG) and, earlier, in the Trusted Computing Platform Alliance (TPCA), HP has been driving efforts to improve trust and security on computing platforms. The first result of these efforts is HP ProtectTools Embedded Security, a security chip with native cryptographic capabilities, available at additional cost as a Configured To Order (CTO) option on HP Compaq business PCs, beginning with the Business Desktop d530.

In addition to ProtectTools Embedded Security, the ProtectTools family of products, features and services offers enterprise security solutions that span multiple technologies and computing platforms.

## **notice**

© Copyright 2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

May 2003  
5981-7667EN

## introduction

With the rapid increase in the amount of information flowing across intranets and the Internet, security has become an essential part of today's computing world. Organizations that fail to protect against viruses, intrusions and other threats may suffer physical losses – such as money, intellectual property or strategic documents – or less tangible but equally damaging losses such as lost business opportunities or a damaged reputation.

Organizations eager to take advantage of the convenience, flexibility and long-term savings inherent in a Wireless Local Area Network (WLAN) implementation face additional security risks. Since user credentials and data are broadcast over a radius of three hundred feet or more from each client machine or wireless access point, an intruder has only to intercept radio waves to threaten an unsecured WLAN.

Whether implementing a traditional or wireless network, today's organization should take steps to minimize losses due to security breaches. It may seem expedient to create a closed architecture to help ensure that transactions are authentic, confidential and complete; however, the global marketplace requires an open security solution that supports barrier-free, instant access to information – 24 hours a day, 365 days a year – without impacting corporate security policies or individual privacy.

Customers need security solutions that do not rely on easy-to-hack software and storage but shift the emphasis to hardware-based security. These solutions should be standards-based, practical and easy to use. HP has taken a leading role in industry-wide security standards groups chartered with developing open, trustworthy computing solutions. The initial HP hardware-based trusted computing solution is ProtectTools Embedded Security.

## security

Security has become a key IT spending priorities as managers attempt to minimize exposure to expensive security breaches.

- 90% of respondents to an FBI survey had detected computer security breaches within a twelve-month period.
- One stolen notebook computer can cost an organization as much as \$89,000.
- 85% of large organizations were attacked in 2002.
- The "I Love You" virus alone cost organizations \$8.75 billion<sup>1</sup>.

---

<sup>1</sup> CSI/FBI Computer Crime and Security Survey, [Computer Security Institute](#), 4/7/2002; [CERT Annual Report](#), 2002; [Mi2q](#) Intelligence Briefing, 10/25/2002

Table 1 shows that multiple business areas are at risk from security breaches.

**Table 1. Potential risks**

<b>Business area</b>	<b>Risk</b>
Information privacy	<ul style="list-style-type: none"><li>• Lost revenue and value</li><li>• Lost competitive advantage</li><li>• Reduced public confidence</li></ul>
Application availability	<ul style="list-style-type: none"><li>• Operational downtime</li><li>• Repair and recovery costs</li></ul>
Asset vulnerability	<ul style="list-style-type: none"><li>• Lost physical and intellectual assets</li></ul>

As shown by Table 1, there is a huge, very public potential for loss – security flaws have become newsworthy! Businesses need a robust, simple end-to-end security solution that protects IT resources: network security, data, communications and client devices.

## conventional security solutions

Conventional security solutions focus on one or more of the following areas: user authentication, secure communications and data protection, achieving varying levels of success. However, even in a network with well-implemented security, client devices are often poorly protected and may still represent a weak point – particularly when remote users attempt to log on to the corporate network.

A key objective of a conventional security solution is user authentication – ensuring that users are authorized to access network resources. A variety of authentication methods is available, including the use of passwords, Smart Cards or biometric ID systems. However, passwords are typically easy to hack while “strong” passwords require significant hands-on management. A more robust solution could offer an additional security layer such as platform authentication, with secure, easy-to-manage, tamper-resistant credential storage. Combining multiple authentication layers can significantly strengthen security.

After authentication, the next objective is to secure communications by encrypting session data. However, to maximize network throughput, encryption methods can be less than robust, making the data relatively easy to hack – indeed, any encryption method that relies entirely on software is subject to hacking. A more robust solution could offer a securely stored key (a root key), used to encrypt or decrypt all other encryption keys, making communications much more difficult to hack.

Lastly in a conventional security solution, sensitive data are protected through measures such as user authentication, encryption and anti-virus software. As indicated above, current user authentication methods are not robust; in addition, IT managers cannot be certain that client devices connecting to the network are running the appropriate anti-virus or firewall software. Platform authentication can help ensure that any client platform is configured correctly and is running appropriate software.

## trusted computing standards

Development of trusted computing standards was initiated by the **Trusted Computing Platform Alliance** (TCPA), an industry working group formed in 1999 by HP, Compaq, IBM, Intel, and Microsoft. The objectives of the TCPA were twofold:

- To collaborate with hardware, software, communications, and security technology vendors to create a specification for a cross-industry, trustworthy platform that can improve the security of Internet-based communications and commerce
- To promote the adoption of the TCPA specification by making the solution affordable, interoperable, and adaptable

To meet these goals, TCPA planned to develop standardized building blocks that would establish trust throughout – and beyond – the enterprise. The first building block offering platforms a root of trust, the trusted computing platform (TCM), was defined in [TCPA Main Specification 1.1](#), released in July 2001.

### Trusted Computing Group

An evolutionary follow-up to TCPA, the [Trusted Computing Group](#) (TCG) carries on the work begun by TCPA. While organizational goals have not changed, there have been key changes in organizational structure and membership. Initial TCG founding promoters HP, IBM, Intel, Microsoft and AMD plan to accelerate the creation of open<sup>2</sup> standards while streamlining adoption.

TCG expects to attract a broad, diverse membership<sup>3</sup> driving open trusted computing standards.

## hp ProtectTools Embedded Security

HP ProtectTools Embedded Security and HP ProtectTools Embedded Security Manager technologies result directly from the HP involvement with trusted computing standards. These technologies provide building blocks that can interact with other ProtectTools products to offer end-to-end solutions for asset protection, asset control, data protection and network security. (Refer to Appendix A for more information on the ProtectTools family of products.)

---

<sup>2</sup> History suggests that the widespread adoption of a new technology is most successful when based on open standards.

<sup>3</sup> TCPA attracted almost 150 members; most are expected to join TCG.

## overview

- ProtectTools Embedded Security is a hardware module<sup>4</sup> (security chip) that is deployed on the motherboard of the business desktop.
- ProtectTools Embedded Security Manager software has two key functions:
  - Controlling the basic operation of ProtectTools Embedded Security (enabling, ownership, and more)
  - Providing simple file and folder encryption

## ProtectTools Embedded Security



ProtectTools Embedded Security features a TCGA 1.1-compliant hardware security chip from [Infineon Technologies](#) that integrates the core elements into the platform.

Each ProtectTools Embedded Security chip<sup>5</sup> is unique and is bound to a specific system. Each performs key security processes independent of other platform components (such as processor, memory or operating system).

Key capabilities of ProtectTools Embedded Security include:

- Platform authentication – An organization should be able to authenticate any platform attempting to connect to the network and control the access rights of network users. Further, the organization can help ensure that the platform cannot compromise network integrity. The reverse also applies; a client device should be able to trust the network – a client receiving a remote management task should be able to authenticate the platform that issued the request.  
ProtectTools Embedded Security lays a foundation for these levels of trust.
- Protected storage – Today's users often store sensitive information such as IDs, passwords, encryption keys or digital certificates in easy-to-hack locations (for example, as cookies or in the system registry on Microsoft Windows operating systems). ProtectTools Embedded Security encrypts<sup>6</sup> this credential information using a root key that is stored in silicon, making the encrypted credentials almost impossible to compromise.  
In addition, ProtectTools Embedded Security can protect local files and folders, encrypting these data with keys created from the root key.

---

<sup>4</sup> A Trusted Platform Module (TPM)

<sup>5</sup> ProtectTools Embedded Security is compatible with any application using the Microsoft Cryptographic Application Programming Interface.

<sup>6</sup> With 2048-bit RSA public key encryption

- Data integrity – To secure data from hackers, ProtectTools Embedded Security offers hardware-based key generation, encryption, decryption and digital signature operations for applications such as secure network logon, digitally signed e-mail and secure website access. Further, ProtectTools Embedded Security protects local data for single log-in applications<sup>7</sup>
- Privacy – The security enhancements delivered by ProtectTools Embedded Security further protect the user's privacy. Moreover, platform authentication with ProtectTools Embedded Security does not rely on an identification that can be tied to a particular platform or user<sup>8</sup>.

## PC implementation

ProtectTools Embedded Security and ProtectTools Embedded Security Manager are available as Configured To Order (CTO) options.

A ProtectTools Embedded Security-enabled platform complements and enhances the security capabilities inherent in the Microsoft® Windows® 2000 or Windows XP® operating system. For example, while the operating system can encrypt local files and folders based on an Embedded File System (EFS), ProtectTools Embedded Security offers an additional layer of security by creating encryption keys from the platform's root key, which is stored in silicon. This process is known as "wrapping" the encryption keys.

Further, ProtectTools Embedded Security can complement authentication technologies such as Smart Card or fingerprint ID to provide another layer of security. Since many organizations rely on passwords alone for authentication, ProtectTools Embedded Security is a robust, easy-to-implement solution for strengthening security.

## extending trust – throughout the platform

ProtectTools Embedded Security can extend trust throughout the platform – from the BIOS to applications – in the following sequence:

1. The system powers on.
2. The BIOS communicates with ProtectTools Embedded Security to verify that the BIOS can be trusted.
3. The BIOS queries the user for authorization to use the platform.
4. The BIOS communicates with the operating system (OS) loader and ProtectTools Embedded Security to verify that the OS loader can be trusted.

---

<sup>7</sup> Single sign-on applications do not require an additional log in (unlike applications behind an internal firewall or those that use a shared folder, for example). Protected storage is available for Microsoft Word or Microsoft PowerPoint files, or general Web pages, for example.

<sup>8</sup> ProtectTools Embedded Security creates a hash (attestation) of the current configuration of the platform, which is used for authentication purposes.

5. The OS loader communicates with the OS kernel. When the kernel loads, it is aware of any software that has already had access to the system. The OS kernel now has total control of the platform.
6. The OS kernel extends trust to applications.

Access to data and other sensitive information on the platform may be denied if the boot sequence does not proceed as expected.

## extending trust – to the network

ProtectTools Embedded Security can extend trust from the platform to the network.

In the following two scenarios, a hacker is attempting to log on to a corporate network. Figure 1 shows what can happen if the server is required to authenticate a PC that is not ProtectTools Embedded Security-enabled.

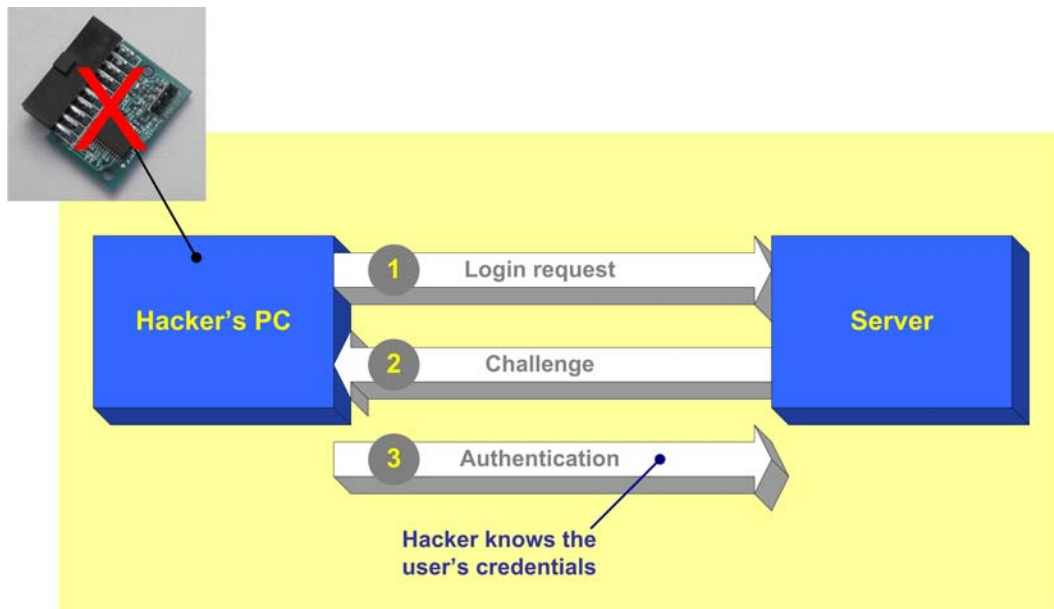
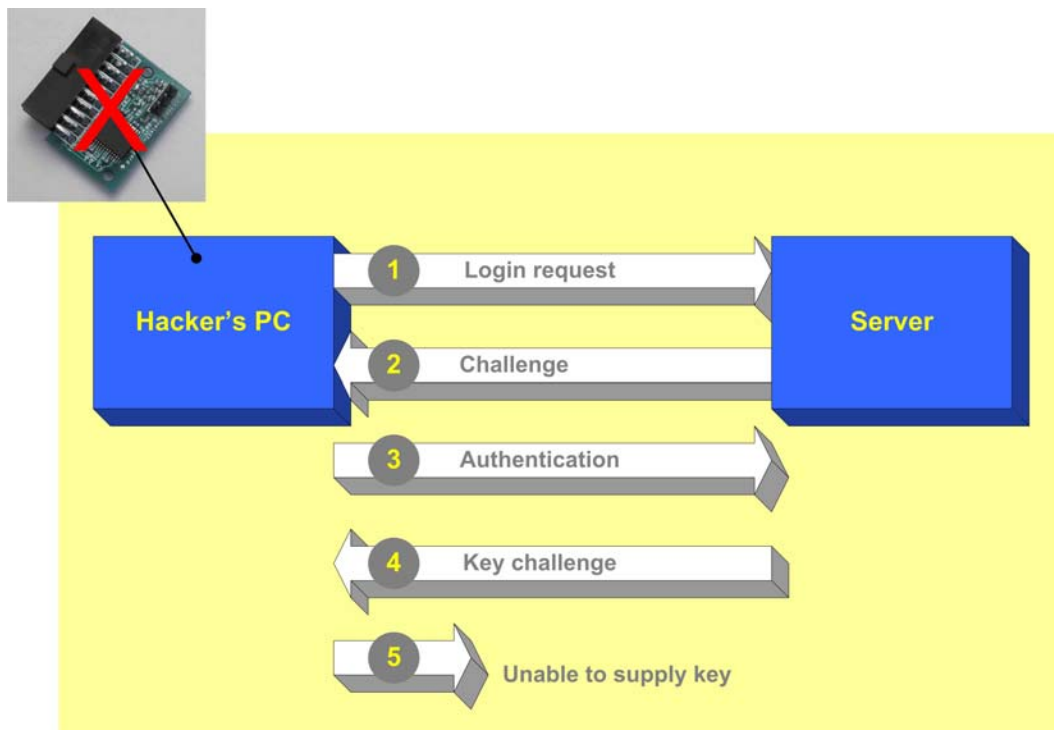


Figure 1: A hacker attempting to log on to the network – no ProtectTools Embedded Security

If the credentials of an authorized user are known, a hacker may be able to log on to the network.

Figure 2 shows what can happen if the server is required to authenticate a ProtectTools Embedded Security-enabled PC.



**Figure 2: A hacker attempting to log on to a network that is protected by ProtectTools Embedded Security**

Even if the hacker is able to supply appropriate user credentials, the PC is not ProtectTools Embedded Security-enabled so it is unable to respond to the server's key challenge. The server is expecting a challenge response that has been encrypted using an appropriate root key.

---

**Note:** The user's privacy can be maintained during the authentication of a ProtectTools Embedded Security-enabled platform. The credential challenge need not include personal information about the user or the platform; rather than identifying the user, authentication helps to ensure that the platform can be trusted to access specific networks.

---

Almost total control of network access is available using multiple layers of user authentication (for example, a strong password, a Smart Card, a token or biometrics) backed by the platform authentication offered by a ProtectTools Embedded Security-enabled PC.

## sample scenarios

The following scenarios briefly illustrate benefits of using ProtectTools Embedded Security.

### delivering strong authentication

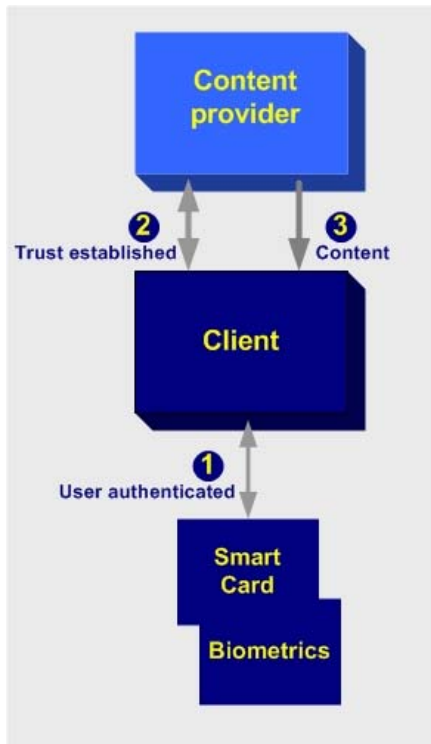


Figure 3: Strong authentication

Today's IT managers face serious authentication issues while the threat of viruses reduces the level of trust within the network.

Figure 3 shows a solution that incorporates multiple layers of authentication: ProtectTools Embedded Security and an access control device (such as a ProtectTools for Smart Cards or biometrics).

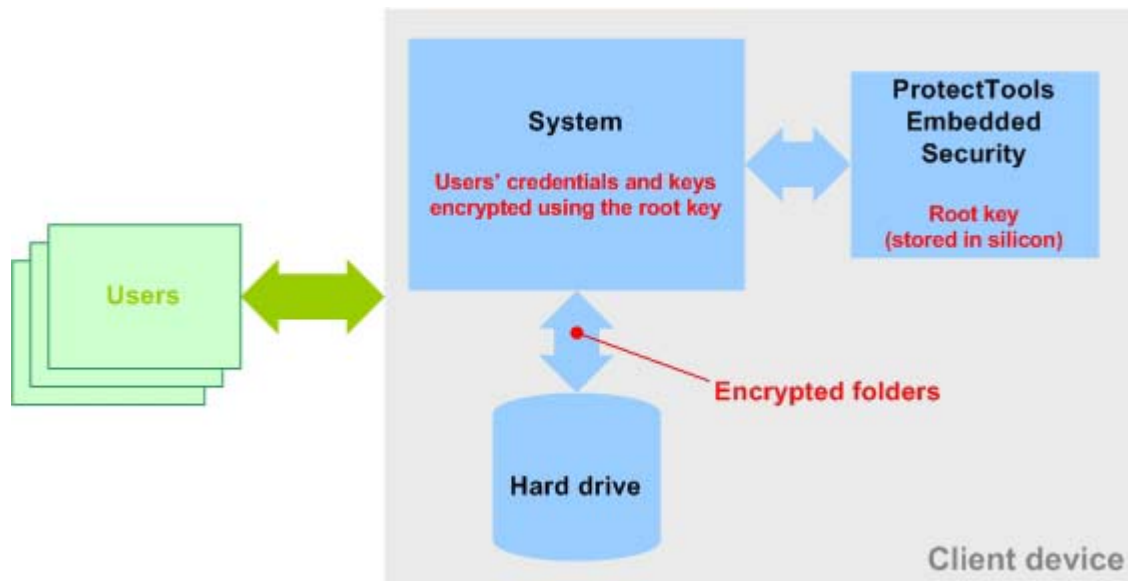
The client first requires a Smart Card or biometrics to authenticate the user. Next, the ProtectTools Embedded Security-enabled client demonstrates to the content provider that it can be trusted – its hardware and software are configured appropriately. Further, the content provider can require the client to supply a hardware-protected, verifiable digital signature.

After authenticating the client platform, the content provider delivers the desired content.

## securing data storage for multiple users

Multiple users on a single client device (whether a desktop PC or mobile device) may need individual, secure access to locally-stored data. Further, the organization would prefer hardware rather than software storage for the root key used to protect sensitive information such as individual logon credentials and encryption keys.

Figure 4 shows a solution that incorporates ProtectTools Embedded Security.



**Figure 4: Securing data storage for multiple users**

ProtectTools Embedded Security offers secure storage in silicon for the root key needed to encrypt individual credential information and locally-stored data.

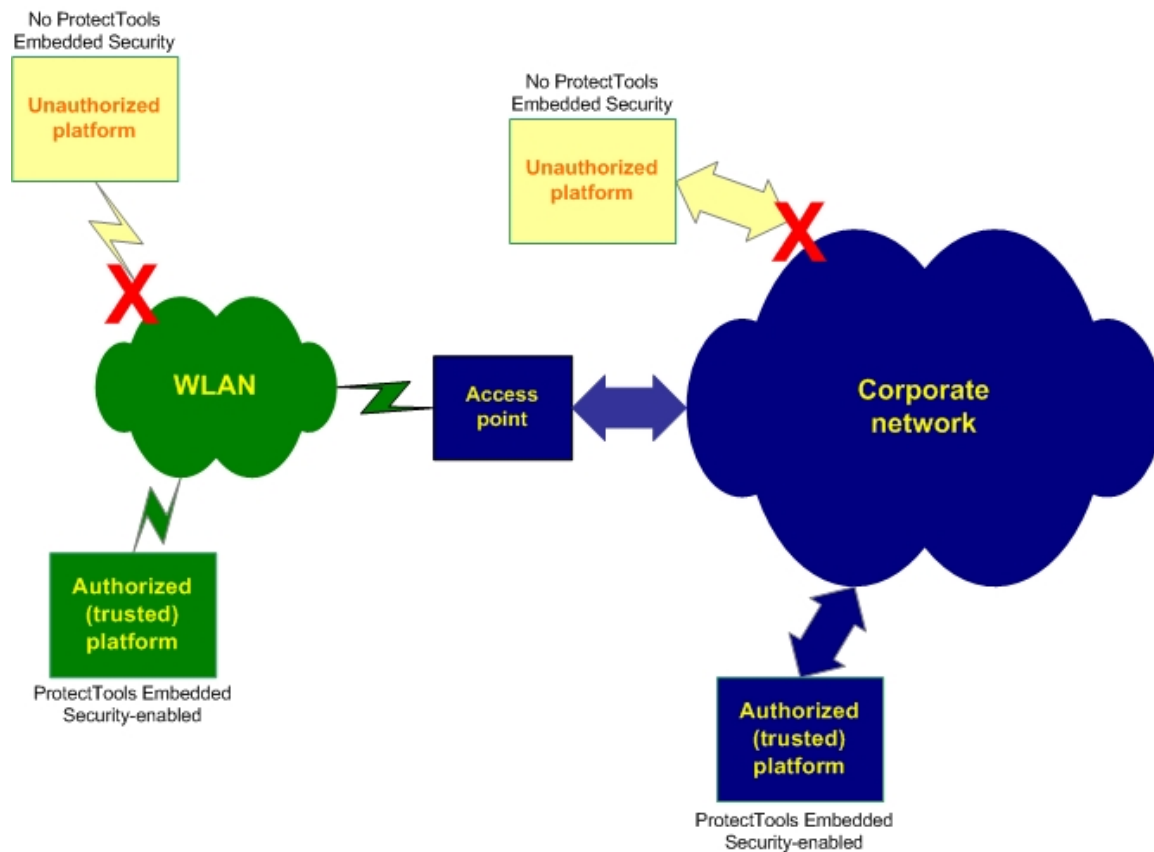
Benefits in this scenario include:

- File or folder encryption that is transparent to the particular user
- Encrypted folders that are invisible to other users on the same client
- Windows-based applications access encrypted files in the same way as conventional files

## providing secure network access

Many organizations have difficulty preventing unauthorized devices or unauthorized device configurations from accessing the corporate network. This risk is increased when radio signals from wireless networks “leak” into surrounding, publicly-accessible areas.

Figure 5 shows a solution that incorporates ProtectTools Embedded Security.



**Figure 5: Preventing unauthorized network access**

A unique root key identifies each ProtectTools Embedded Security-enabled client machine as a platform to be trusted on this network. Other benefits include:

- Helping lay the foundation for more secure network access to traveling employees
- Can help restrict network access through wireless access points to trusted platforms

---

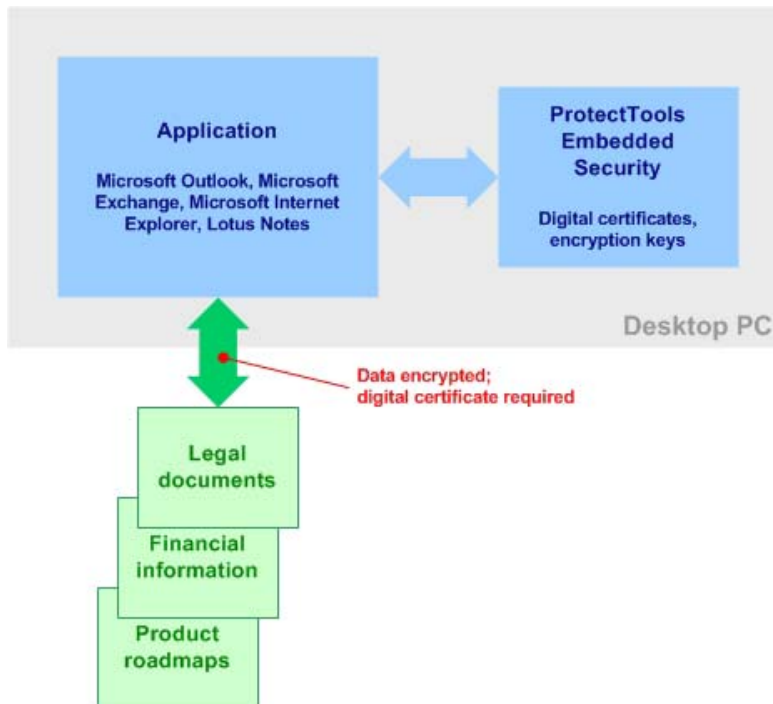
**Note:** As demonstrated by this scenario, ProtectTools Embedded Security can help strengthen WLAN security.

---

## restricting access to confidential information

In many organizations, access to confidential information must be restricted to a limited audience.

Figure 6 shows a solution that incorporates ProtectTools Embedded Security.



**Figure 6: Restricting access to confidential information**

ProtectTools Embedded Security offers secure storage for the root key needed to decrypt digital certificates and other encryption keys. Credentials and keys are less vulnerable to attack.

## summary

Many current security solutions tend to be software-based and relatively weak, making them particularly vulnerable to hackers. ProtectTools Embedded Security offers an open, hardware-based security solution that is robust, practical and easy to use.

ProtectTools Embedded Security is available at additional cost as a Configured To Order (CTO) option on select business PC platforms from HP.

ProtectTools Embedded Security technology demonstrates the HP commitment to trust, security and privacy, helping to create a strong foundation for e-commerce and other network applications. HP is one of the leaders and supporter of current industry initiatives aimed at achieving secure computing.

## **for more information**

For more information on HP ProtectTools Embedded Security, contact an HP hardware or services sales representative, or visit the HP website at <http://www.hp.com/products/security> .

To learn more about the Trusted Computing Group, visit their website at <http://www.trustedcomputinggroup.org>.

## appendix a – HP security solutions



HP has taken a leading role in secure computing with end-to-end solution offerings for asset protection, asset control, data protection and network security.

### ProtectTools

ProtectTools is a family of products, features and services from HP, offering enterprise security solutions that span multiple technologies and computing platforms (including client PCs). These solutions include but are not limited to:

- ProtectTools Embedded Security and ProtectTools Embedded Security Manager
  - File and folder encryption enhancements to native Windows EFS
  - Personal Secure Drive– a virtual encrypted disk
  - e-mail security with encryption and digital signatures
  - Integration with products that support native Windows cryptographic functions<sup>9</sup>, including:
    - Support for encrypting Microsoft Office macro files
    - Microsoft Outlook, Microsoft Outlook Express
  - Integration with industry-standard cryptographic interfaces such as Public Key Cryptography Standards (PKCS) #11
  - Support for native Netscape cryptographic capabilities
  - Token authentication replacement (such as RSA SecurID)
- ProtectTools Smart Card Security Manager
  - Support for Smart Card-based user logon
  - Pre-boot authentication and integration with DriveLock
- BIOS and device security
- Biometric security

---

<sup>9</sup> Using the Microsoft Cryptographic Application Programming Interface (CAPI)