hp-ux and Windows™ security interoperability

february 2001

white paper

table of contents

introduction

In today's e-business environment the traditional data center role is shifting to a service provider role. As a service provider on the Intranet, or a service provider serving customers over the Internet, security is a critical element. Security enables Internet and Intranet e-business to be conducted. The new security is not about setting up walls to keep people out, but enabling mechanisms to let the right people in and become participants in ever changing virtual teams. Hewlett-Packard highlights the attributes of availability, security, manageability, reliability, scalability, and quick time to solution for e-business infrastructure products and solutions. This paper focuses on the security attribute. It further focuses on security interoperability between the HP-UX operating environment and the Microsoft Windows® (NT® and 2000®) operating environment.

Officers, managers and security professionals should find this marketing paper helpful in determining the interoperability security technologies available from HP. Many if not most e-business providers work with mixed operating systems and mixed infrastructure platforms. For example, Windows client desktop and laptop machines are routed through the Internet or Intranet with HP switches and hubs or Cisco® products and work with Windows and UNIX® HTTP front-end processors, application servers, database servers and into mainframes in legacy data centers. You desire interoperable security solutions among mixed platforms. This preserves investments and facilitates orderly migration strategies as you implement e-business and service provider strategies.

HP systems work with multiple operating systems. Linux®, Windows and HP-UX are interoperable at many levels. But our purpose here is focused on HP-UX and Windows security interoperability. We discuss how secure HP-UX/Windows works with mixed operating environments, to provide the four "A" of security: Authentication, Access control, Audit and Administration.

We will focus on secure interoperability for the e-business infrastructure. Information security and transaction security are also important topics but are not covered in this paper. Provisioning and delivery of security products is also important, but not covered here. Security consulting, secure systems implementation, and secure turnkey operations are also services of HP but are not discussed here.

mixed platforms: hp-ux and and Windows NT need for interoperabillity

It is not surprising that HP-UX/Windows security interoperability is an important issue to both HP and its customers. HP provides worldwide Microsoft®-authorized support with comprehensive multivendor coverage for corporate customers' overall Windows NT needs. HP's complete portfolio of Intel® hardware and Microsoft Windows NT®-based services, including support, disaster recovery, and professional services and training, allows customers to choose the services they need as they deploy business-critical Windows NT-based applications.

HP offers Windows NT Workstation preinstalled on all business-computer lines, including the HP Vectra Corporate PC, HP Kayak® PC Workstation, HP Brio® PC and HP OmniBook® notebook PC. More than half of HP Vectra Corporate PCs are shipped with Windows Workstation NT 4.0 preinstalled. Many of these systems are client machines accessing Windows and HP-UX servers in enterprise systems worldwide.

HP offers industry-leading printers and a wide array of peripheral products that have been certified for Windows 2000. These include mid to high-end storage solutions that are designed to meet customers' NT storage-consolidation requirements.

Windows 2000 is a major development platform for HP OpenView® solutions, which monitor Windows 2000 environments to ensure the health and availability of the operating system and server-based business-critical applications.

> HP's full offering based on Windows 2000 can be found at
> http://microsoft.hp.com/windows2000/

HP is a leader in enterprise infrastructure products that use HP-UX as the primary operating environment. More than 50,000 HP 9000 servers (A-Class though Superdome) are installed and operating in data centers and e-business service providers world wide.

Recently HP announced HP-UX 11i an expanded portfolio of end-to-end Internet-critical software and services to help customers rapidly deploy e-services and profit in today's Internet environment. The new solutions reduce the complexity that enterprises, service providers and Internet start-ups face in building and running highly available, secure Internet environments. This is a major release of the company's UNIX® operating system, HP-UX, with extensive new Internet-enabling technologies, security, networking, performance and availability features, and the new Servicecontrol manageability tool.

hp-ux 11i a secure platform for e-business

core hp-ux security

Security and trust for e-business begins in the Operating Environment (OE), which in its base configuration is the Operating System (OS). From a fundamentally secure and trusted OS, network and data communications trust and security are built. We begin by describing the trust and security built into the HP-UX OEs.

two modes of security in hp-ux

HP-UX can be configured to operate in one of two security modes: Standard Mode, and Trusted Mode. Standard Mode is the default configuration of the OS. HP-UX is C2 Trusted Systems compliant in the optional Trusted Mode. The OS can be converted to operate in Trusted Mode at any time. Trusted Mode is included with HP-UX at no additional charge.

These modes fill two primary market requirements for security: legacy standards-based UNIX and enhanced C2 level trusted systems. These two requirements are mutually exclusive: industry-standard, legacy UNIX is insufficiently secure to meet the requirements of a C2 trusted system. HP-UX in Trusted Mode extends the standard UNIX security model to meet C2 requirements while maintaining compatibility as much as possible with legacy UNIX.

A white paper is available that describes the security features built in to HP-UX. It can be obtained from

http://www.unixsolutions.hp.com/products/hpux/security.html
A table of HP-UX security features can be found at
http://www.unixsolutions.hp.com/products/hpux/security/hpux11_features.html

hp praesidium intrusion detection system 9000

HP's Intrusion Detection System (IDS/9000) alerts you about hackers who have reached the HP-UX 11.x operating environment and are about to do harm in the place most critical to your computing environment like some key components of the operating system and applications.

IDS/9000 concentrates on monitoring and alarming the HP-UX 11.x operating environment. Other products may be used for intrusion detection on the perimeter of your network. This is termed network intrusion detection. However, the Federal Bureau of Investigation says that 70% of attacks are internal. Host intrusion detection is a must for mission critical servers.

Additional information can be obtained at
http://www.hp.com/security/products/ids/
The product number is J5083AA.

hp-ux technologies for security interoperability

LDAP UX integration

Vendors now offer directories that support the Lightweight Directory Access Protocol (LDAP) as enterprises start deploying LDAP directories. As more applications are directory enabled, important tasks such as administration, authentication and authorization are consolidated and centralized. Integrating HP-UX, Windows NT/2000, and Linux and operating systems with directory services enhances the value of the enterprise-deployed directory.

The three listed LDAP technologies are collectively described as HP-UX Integration. These technologies may be implemented individually or collectively.

- Pluggable Authentication Module, PAM_LDAP authenticates HP-UX users using an LDAP directory.
- NIS/LDAP Gateway (also known as YPLDAP). NIS requests are converted into LDAP requests, which retrieve account, group and other NIS information, and reply to the client using the NIS protocol.
- Name Switch Service, NSS_LDAP accesses users account, group and other data via native LDAP.

LDAP support is the latest in the effort to support customer directories. Originally, UNIX account and configuration information was stored in a series of text files. As the need to share this information across systems increased, the first widely accepted product was Network Information Service (NIS). NIS provides network wide management of many UNIX configuration files (e.g., /etc/passwd, /etc/group, etc/services). A NIS master server generates maps based on the configuration files and transfers copies to slave servers. On NIS client systems, operations reading the configuration file are redirected to send a request across the network to retrieve the information from a NIS server. NIS+ was introduced as a successor to NIS to provide greater scalability and security. Now with LDAP directories, NIS offers even greater scalability and manageability.

HP UX integration is available as product number J4269AA. HP-UX customers may also obtain the LDAP compliant iPlanet Directory Server. This product is explained in this document.

Additional information is available at
http://docs.hp.com/hpux/internet/index.html
And a white paper is available at
http://www.unixsolutions.hp.com/products/hpux/hpux11/whitepapers/netsecur.pdf

kerberos support

The Kerberos protocol provides enterprise-wide strong user authentication by validating user passwords without transmitting the password over the network. A central Kerberos server, called the Key Distribution Center (KDC), verifies the user's credential. A HP-UX login can use any Kerberos 5 Key Distribution Center, such as an MIT® Kerberos Server or a Microsoft Windows 2000® Domain Controller. This achieves common authentication functionality in a heterogeneous Intranet that may include other UNIX hosts and Windows 2000 workstations. Furthermore, the HP-UX implementation of Kerberos supports the password-change protocol, which automates the propagation of password changes. These features can significantly reduce administration complexity in a mixed platform environment.

Additional information can be found at www.hp.com, search on the term Kerberos. Your HP account representative can also provide you with a Kerberos Product Brief. In addition, A Kerberos and Windows 2000 White Paper is available by clicking on this link.

HP's Kerberos offering for HP-UX 11.0 and 11i is available through the following three technologies and products.

- Pluggable Authentication Module (PAM) Kerberos, product J5849AA
- Kerberos client libraries and utilities included in core HP-UX 11.i and in J5849AA for HP-UX 11.0
- The Generic Security Services Application Program Interface, GSS-API included in core HP-UX 11.i. and in J5849AA for HP-UX 11.0. GSS-API has wider use for programmers than just Kerberos services.

pluggable authentication module (PAM) kerberos

HP-UX provides Kerberos authentication as part of the Pluggable Authentication Module (PAM) architecture specified in RFC 86 of the Open Group. With PAM, a configuration file determines which authentication module to use. PAM provides combinations of authentication mechanisms with different levels of security strength and is easily configurable without a system reboot.

PAM Kerberos interoperates with a KDC operating on either a UNIX server or a Microsoft Windows 2000® server. HP-UX 11.i includes the following Kerberized Secure Internet Services (SIS): ftp, rcp, rlogin, telnet, and remsh utilities. When secure Internet services are enabled, all of these commands use Kerberos for authentication.

kerberos client libraries and utilities

PAM Kerberos (J5849AA) for HP-UX 11.0 includes PAM Kerberos, GSS-API and KRB5 client libraries compatible with the MIT reference implementation. For HP-UX 11i, the same product number J5849AA provides the PAM Kerberos, with GSS-API and Kerberos libraries moved to the core operating system. The Kerberos utilities can be linked in either 32- or 64-bit mode and include the following tools:

- **kinit** obtains and caches the ticket granting ticket (TGT) and login-session key.
- **klist** lists the tickets and associated session keys in the credentials cache.
- **kdestroy** removes a principal's login context and associated credentials.
- **kpasswd** manages the user passwords and the corresponding long-term keys stored by the KDC.
- **ktutil** maintains the keytab files.
- **kvno** returns the revision number.

This technology is available in the core HP-UX operating system version 11 and version 11i.

generic security services application program interface (GSS-API)
The Generic Security Services Application Program Interface, GSS-API, provides security services for client/server applications independent of various underlying communication protocols. The services include authentication, integrity, and confidentiality of data. Using GSS-API the system administrator can configure the quality of protection to use for an application with no modification at the application level. The GSS-API is a standard and specified in RFC 2743 of the Internet Engineering Task Force (IETF).

common internet files system (CIFS)

The Common Authentication Technology working group of the IETF has defined several cryptographic mechanisms to implement the security services provided by GSS-API. These are transparent to applications. The use of Kerberos as a GSS-API mechanism is specified in RFC 1964 of the IETF.

GSS-API provides secure communication between two peers with a security context established between the peers. The context is established by an exchange of tokens. When Kerberos is used as the underlying cryptographic mechanism, the client sends a token to the application server that includes a service ticket and an authenticator. If mutual authentication is required, the application server sends a token to the client comprising the application server's authenticator. The GSS-API libraries on the two hosts are responsible for creating and processing the tokens, but the application is responsible for transporting the tokens between client and server.

HP-UX 11i provides GSS-API libraries, including the Kerberos mechanism, as part of the OS core. These libraries can be linked with either 32- or 64-bit applications.

A white paper is available at
http://www.unixsolutions.hp.com/products/hpux/hpux11/whitepapers/netsecur.pdf

hp's CIFS/9000-completing the path to Windows/UNIX interoperability
CIFS/9000 gives HP-UX 11i the best UNIX and Windows interoperability story in the industry. CIFS/9000 gives UNIX and Windows, for the very first time, scalable, secure interoperability that is tightly integrated with the UNIX environment. This means that Windows platforms can now be file servers for HP-UX 11 systems. Additionally, HP-UX 11 systems can now be file servers and print servers for Windows platforms. All with file-serving technology that is tightly integrated with HP-UX and works with standard HP-UX 11 utilities such as OmniBack® and Legato®.

hp-ux 11 integrated with Windows user authentication
HP-UX 11 can be integrated with Windows user authentication because CIFS/9000 delivers UNIX-client-to-Windows-server capability. With CIFS/9000, both Windows and HP-UX 11 platforms can authenticate against Windows domain controllers using the NTLM, making possible common and global user authentication between UNIX and Windows platforms. The Common Internet File System and CIFS/9000 satisfy the need for a common data access method between application servers and Web content servers.

pluggable authentication module
Pluggable Authentication Module NT LAN Manager (PAM NTLM) authenticates HP-UX users against a Microsoft Windows NT 4.0 domain controller using the NT LAN Manager protocol. This product is included in the CIFS/9000 client.

Information can be obtained on this product, which is product B8724AA CIFS/9000 Client for servers and workstations. Additional information is contained at
http://www.unix.hp.com/operating/hpuxcifs9000/infolibrary/documentation/
and http://www.unix.hp.com/operating/hpuxcifs9000/

hp praesidium common data security architecture (CDSA)

The Common Security Architecture is a set of application program interfaces (APIs) to perform cryptography and other public key infrastructure operations. Additional shared libraries implement the API functionality. The Cryptographic Service Provider (CSP) module implements most popular cryptographic algorithms. The actual cryptographic algorithms must be obtained from third-party vendors. The Certificate Library (CL) module implements X.509v3 certificate operations. The Trust Policy (TP) and Data Storage Library (DL) are not implemented in this release. CDSA consists of the most popular cryptographic algorithms needed for security applications; the code may be used by C or C++ applications.

CDSA changes the way software developers can approach writing and disseminating commercial security applications. HP's license agreement allows developers to write applications that make free use of CDSA and to market the application as a product without paying royalties. The code is available on HP platforms on a right-to-use (not right-to-distribute) basis. HP places no limitations on how the cryptographic libraries can be used, in that any application can link to it or use it, royalty-free. Large and small developers alike benefit from the likelihood that the CDSA cryptographic APIs will become pervasive through their adoption by the Open Group.

Application developers will benefit from the portability of code written using CDSA APIs. An application written with CDSA APIs and linked against a CDSA library on a particular platform could be moved to any other platform as long as the other platform has the appropriate CDSA library. No code would have to be modified to make use of the same cryptographic capabilities or functionality. As long as the other system has CDSA, you would simply have to recompile. U.S. application developers implementing CDSA may need to seek U.S. government approval for the export or re-export of their products due to the export control nature of certain cryptography technologies and implementations. In addition, the import and use of certain products with cryptography in some countries may require local country authorization. You should consult with proper government authorities or your legal counsel before distributing your products with cryptography.

A white paper is available at
http://docs.hp.com/hpux/onlinedocs/internet/CDSA.pdf
A press release is at
http://www.hp.com/security/press/releases/19990616-cdsa/
The product number is J4262AA.

hp-ux products for security interoperability

iPlanet® (Netscape®) directory server

The iPlanet Directory Server operates as a central repository of user data controlling preferences, access rights, and security levels. Designed for e-commerce deployments, the directory helps enable companies to manage user names, passwords access control and security authorization for their customers, suppliers, partners and employees.

HP makes available at no additional charge to HP-UX customers the iPlanet (Netscape) Directory Server. All customer company internal employees and regular contractors are licensed to use the directory at no charge. When extranet or outside vendors, contractors or partners are added to the directory, a license fee is required. The Netscape and iPlanet names are now used interchangeably. However, the name will be changed to iPlanet Directory Server with the introduction of version five of the server. The server available to HP-UX customers is the same one described at the iPlanet web site located at http://www.iplanet.com/products/infrastructure/dir_security/dir_srvr/

Netscape Directory Server provides the centralized directory service upon which your Intranet or extranet is based. Netscape servers and other directory-enabled applications use the directory service as a common, network-accessible location for storing shared data such as user and group identification, server identification, and access control information.

The directory service is interoperable with multiple operating environments. For example employees stored in the directory using Windows desktop PCs may pass through the directory for authentication and access control to services, files, and resources running on HP-UX application processors or HP-UX database servers.

The iPlanet directory service is used to store virtually unlimited types of information. For example, a directory service can be thought of as an electronic telephone book in that it contains personal contact information such as a person's name, telephone number, mail address, office number, and so forth. But a directory server goes beyond this usage by allowing the enterprise to store other types of information such as:

- Physical device information (e.g., you can store information about all the printers in your organization, where they reside, whether they are color or black and white, their manufacturer, date of purchase, serial number, etc.).
- Private employment information such as salary, government identification numbers, home addresses and phones numbers, pay grade, and so forth.
- Contracts or accounts information, such as the name of the client, final delivery date, bidding information, contract number, and milestone due dates.

how it integrates hp-ux and Windows NT, Windows 2000

Extensive meta-directory capabilities allow easy integration with existing infrastructures. Data from disparate enterprise systems is synchronized within the directory and can be easily integrated into new applications that also support the Lightweight Directory Access Protocol (LDAP). Since Windows Active Directory Services® is also an LDAP compliant directory the two directories can interoperate using the LDAP UX integration v1.2 product.

The directory provides a standard method, via LDAP, for applications to access legacy data. This "virtual directory" enables a client to make a request to the iPlanet Directory Server to retrieve information from an existing database. In this way, the data remains in its original database, but is accessed by a standard LDAP request.

Additional information is available at
http://docs.hp.com/hpux/internet/index.html

The Directory Server is provided at no additional charge to HP-UX customers. The product number J4264AA for USA/Canadian customers and J4258BA for international customers are available on the web at www.software.hp.com

kerberos server

Hewlett Packard references CyberSafe Corporation, a leading provider of secure Internet and client/server communications.

The Kerberos Server offered by CyberSafe is named ActiveTRUST Enterprise Edition. It is an enterprise security solution featuring interoperability with the Kerberos authentication protocol included in Windows 2000. ActiveTRUST Enterprise Edition allows organizations with mixed system environments to extend their existing security infrastructures to include Windows 2000 security, providing a single and central source of enterprise-wide authentication and security management. With any combination of clients and security servers from CyberSafe or HP-UX and Microsoft, authorized users have the flexibility to logon with a single identity from any CyberSafe-supported platform, including HP-UX, Windows 9x and Windows NT.

Any organization that supports multiple platforms and applications must deal with issues of interoperability. With Windows 2000, Microsoft utilizes Kerberos an open standard security protocol. When considering the introduction of Windows 2000 to a mixed system environment, and the CyberSafe ActiveTRUST security solution for enterprise interoperability within that environment, there are generally five key topics to evaluate: interoperability, deployment, administration, single sign-on solutions, and SSPI to GSS-API.

interoperability

Users can pass seamlessly between environments without effort or notice. Through cross-realm authentication and single sign-on, the services of both Windows 2000 and the ActiveTRUST solution are available to users. Realms, or domains, are groupings of machines generally defined by business functions, much like sub-domain names within an organization. A heterogeneous organization typically contains different realms, each reflecting a business unit's particular resources, functions, and policies.

SSPI and GSS-API

Microsoft's security API, Security Support Provider Interface (SSPI), is wire-level compatible with GSS-API, the security standard used in the ActiveTRUST solution for securing applications. Interoperability here means SSPI and GSS-API clients and servers will work with one another. HP-UX GSS-API implementation is compatible with Microsoft SSPI when the Kerberos mechanism is used.

Additional information White Papers can be obtained from CyberSafe by clicking here.

hp praesidium IPSec/9000

main features of IPSec/9000

Hewlett-Packard's IPSec/9000 is a software product that supports elements for network security such as authentication, confidentiality, integrity, non-repudiation, packet filtering, management and administration with access control. It features Internet Key Exchange (IKE) support.

The IPSec product is built on industry-defined standards and is designed to provide interoperable, high quality, cryptography-based security for IP traffic. IPSec/9000 runs on HP 9000 S700 and S800 systems with HP-UX 11.x, HP-UX 11i and all subsequent releases. It is available in either 56-bit DES or 168-bit 3DES versions.

convenient security

IPSec/9000 is not bundled with any particular security product. Instead it is a generalized security product that provides security customized according to configurations and profiles defined by the user or customer. It actually allows the user to determine what applications he or she wants to secure. Moreover, IPSec/9000 provides security that is transparent to user applications. Applications do not have to change to use the security features provided by IPSec.

Once IPSec/9000 is installed, the user can enable or disable it without having to reboot or reconfigure the HP-UX system that is running. The user also has the capability of using IPSec/9000 Policy Manager to define which type of applications will and will not have secure channels of communications, and to specify the level of security given to these secure channels.

end-to-end or gateway configuration

IPSec/9000 provides a secure encrypted user session between two systems running HP-UX. This feature is configured transparently to user applications via a policy configuration file supplied by the Security Administrator using the IPSec/9000 GUI.

IPSec/9000 can reside either at an end-node or (in a future release) a gateway node, thus providing support for end-to-end or gateway configurations. This flexibility gives the user the ability to define security over the open Internet, over an Intranet, or both.

interoperability by design

IPSec/9000 is built on industry standards as defined by the IETF IPSec working group. Abiding by this standard allows IPSec/9000 to interoperate with non-HP machines abiding by this standard. IPSec/9000 has been able to interoperate with more than 25 other IPSec implementations including Microsoft Windows 2000® IPSEC. Furthermore, when IPSec/9000 is enabled, it is designed to not adversely affect users, hosts, and other Internet components that do not employ IPSec to protect their traffic.

additional Information

Additional information is located on the HP web site at www.hp.com. Search on IPSec. Or you can click here for additional information

putting it all together

security interoperability chart explained

The security interoperability chart on the following page provides a convenient method to determine interoperability between a source resource and a destination resource. The far-left column identifies the Hewlett Packard security product or technology that enables the interoperability. The four right most columns identify the primary security functionality provided by the product or technology. This chart may be helpful as a quick reference for security interoperability.

directory case study

A growing number of companies are implementing enterprise-wide directories as key building blocks of their integrated systems architectures. These directories unify scattered proprietary systems, give users easier access to computing resources and lay the groundwork for interconnected applications that support the gamut of apps, including ecommerce and supply-chain business processes. For example, a company wanting to bring together business partners and suppliers in an integrated chain needs a unified directory to track users, system resources and data traversing the companies' interconnected networks. And the great move to E-business requires directories that let companies securely carry out thousands of Web transactions every hour. The directory must be standards-based to ensure all partners and customers can access it, and it must be scalable. Netscape Directory Server is compliant with the LDAP v3 specification. An excellent example of this is Ford Motor Company's use of Netscape Directory Server as the foundation for the Ford Supplier Network, an Extranet that lets Ford deliver information and applications to Ford's suppliers around the world. With more than 200,000 directory entries for people and other resources stored in a central directory, their need to simplify administration and reduce cost of ownership is handled by Netscape Directory Server.

cross realm interoperability

Some organizations operate with two realms, Windows for presentation and client's services and HP-UX for serving applications and databases. With HP interoperability solutions both realms can securely interoperate. For example, using the CIFS facilities a Windows client can be authenticated to an HP-UX Server. Or the Windows client can access the iPlanet Directory Server for authentication and access control. In a similar manner, an HP-UX client gains access to a windows server using CIFS.

The Windows realm may be operating with Windows Active Directory Server (ADS) and the HP-UX realm may have iPlanet Directory Server installed for Authentication and Access control. Using LDAP UX integration HP-UX clients or server can access the ADS and can access the iPlanet directory natively. By utilizing PAM Kerberos, HP-UX Clients and servers can access any standard Kerberos KDC.

There are many additional combinations of interoperability. View the Security Interoperability Chart to determine the interoperability combination that fits you requirements.

product or	interoperability		security functionality			
technology	source	destination	authentication	access	administration	audit
Common Internet File System (CIFS)	HP-UX client	Windows server			●	
Common Internet File System (CIFS)	Windows client	HP-UX server			●	
Common Internet File System (CIFS)	HP-UX client or server	Windows NT domain controller	●			
Common Security Architecture (CDSA)	HP-UX client or server	Application software	●	●	●	●
Common Security Architecture (CDSA)	HP-UX client or server	Higher-level security protocols	●	●	●	●
GSS-API	HP-UX client or server	Application software	●		●	
GSS-API	HP-UX client or server	Any Kerberos KDC (RFC1510)	●		●	
HP-UX 11, 11.I	HP-UX client or server	HP-UX client or server	●	●	●	●
IDS/9000	HP-UX client or server	HP-UX client or server				●
iPlanet Directory Server	HP-UX client or server	iPlanet directory	●	●	●	
iPlanet Directory Server	Windows client	iPlanet directory			●	
IPSec/9000	HP-UX client or server	Any standard IPSec product	●	●	●	
IPSec/9000	HP-UX client or server	HP-UX client or server	●	●	●	
IPSec/9000	Windows 2000 client	HP-UX client or server	●	●	●	
IPSec/9000	HP-UX client or server	Windows 2000 client	●	●	●	
LDAP UX Integration NIS Gateway	HP-UX NIS Service	Any LDAP directory	●		●	
LDAP UX Integration NSS LDAP	HP-UX client or server	Any LDAP directory	●		●	
LDAP UX Integration PAM LDAP	HP-UX client or server	Windows active directory	●	●	●	
LDAP UX Integration PAM LDAP	HP-UX client or server	iPlanet directory	●	●	●	
LDAP UX Integration	HP-UX client or server	Any LDAP directory	●		●	
LDAP UX Integration	iPlanet Directory	Windows active directory	●		●	
PAM Kerberos	HP-UX client or server	Windows 2000 Kerberos KDC	●		●	
PAM Kerberos	HP-UX client or server	Any Kerberos KDC (RFC1510)	●		●	
PAM NTLM	HP-UX client or server	Windows NT domain controller	●		●	

This chart can be read as follows: The product or technology can be used by the source resource to inter-operate with the destination resource. Additionally, the product row also provides the security functionality in the column marked with an "x". An example is: an HP-UX client or server to access Windows Active Directory can use the pluggable authentication module (PAM) Kerberos. This provides the security functionality of authentication, access control and administration.

i n v e n t

All brand names are trademarks of their respective owners. Technical information in this document is subject to change without notice.
© Copyright Hewlett-Packard Company 2000. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws. 2/2001