

# HP-UX 11 Security

## Overview<sup>1</sup>

This document describes the security-related features and benefits of the HP-UX core operating system. Releases described in this document include HP-UX 10.20, and 11.0. The special, high-security OS releases such as 10.09, 10.16, and the Virtual Vault operating systems are not described here. This document is organized as follows:

- 1) Section 1 contains the overall purpose and organization of this paper.
- 2) Section 2 contains OS security concepts which define the terms used and scope of Operating System Security.
- 3) Section 3 contains a description of available security features in the two modes (Standard and Trusted), how security is managed through SAM, NIS, and NIS+. At the end of the section is a table of HP-UX features and their associated customer benefits
- 4) Section 4 is a summary of security features available by release (10.20, 11.0, ...)
- 5) Section 5 provides additional reference information for further study.
- 6) Appendix A provides the specifications and availability of the CDSA Cryptography.

## Security Programs Not Covered in This Document

Hewlett Packard has numerous activities in security outside of core operating systems, including:

- Praesidium, the HP program and brand name for security infrastructure middleware. Information on these products can be found in <http://www.hp.com/go/security>
- HP offers Versecure, HP's patented hardware-based cryptography framework that meets the security needs of a global marketplace. Further information on this program can be found in <http://www.hpconnect.com/versecure>

---

<sup>1</sup> By Mike Jerbic, Hewlett-Packard Company, [mjeric@cup.hp.com](mailto:mjeric@cup.hp.com), 408-447-6299

## OS Security Concepts

Every technical field has its own vocabulary and set of baseline concepts. This section defines the terms used in this paper. As much as possible these concepts, terms, and definitions have been derived from widely relied upon references. An understanding of these terms and concepts is required before a presentation of HP-UX security features. HP-UX implementation of these security concepts is described in Section 3.

### Identification and Authentication

Identification refers to the naming of each user on the system. Secure systems require that each user has his/her own unique identification. In UNIX, this is an eight-character maximum user name and corresponding numeric userid.

Authentication refers to the proof that the user is who he/she says he/she is. This is usually done through a password that is known only to the user, although other stronger mechanisms exist such as two-factor authentication, in which a token (smartcard) is used along with a PIN. Smartcard authentication requires the user both to have the smartcard and to know the PIN in order to access the system

The strength of an authentication system is frequently an issue with trusted systems. Password length and complexity are figures of merit for a cracker-resistant password. Features such as password lifetime controls force users to change their passwords periodically. Because the divulging of a password allows access to the system, password and user account management are often focus areas for security administrators.

### Authorization

The authorization mechanism in a system grants privileges to individual users. In the UNIX operating system, authorization is divided into two user classes: root users (also known as superusers), who have authorization to do almost anything to the system including bypassing security controls, and regular users, who have no privileges other than ordinary access to programs and data. Root users have authorization to administer the system, perform backups, and bypass security controls.

Fine-grained authorization that separates an all-powerful root user's power into separate authorizations goes by many names: administrative roles, least privilege, etc. In general, UNIX systems do not support these kinds of authorization models, however, through clever usage of existing security features, some separation of privilege can be approximated with HP-UX.

### Access Control

A system's access control mechanism mediates user access of system resources (files, printers, programs, etc.). UNIX access controls take the form of two mechanisms: standard UNIX file permissions (read, write, execute granted on a user, group, other basis) and Access Control Lists.

Access Control Lists are file-specific (that is, each file will have an ACL) and mediate that file's access to a finer granularity than standard UNIX permission bits. ACLs grant read, write, and/or execute permissions to a specified list of users. ACLs can also specify a group of users who specifically don't have access rights to the file.

### Audit / Accountability

The audit system can be configured to log events that root and ordinary users do with the system. In the most extreme case, all security-relevant events are logged. The performance overhead of this extreme auditing may be impractical, so usually only events that are particularly relevant to the server's application or the customer's business environment are logged.

**Object Reuse**

For a system to be secure, it must guarantee that a newly created object (memory buffer, file, etc.) does not contain information "left over" from the last time it was used. The 'object reuse' requirement of a secure system simply states that all user accessible resources are initially cleared or otherwise initialized so that no lingering information can be extracted from them.

**Assurance**

The above concepts (2.1-2.5) are features of an operating system. Features themselves are not enough to determine the security of a system. Assurance that the system's security features work as advertised is required for some applications, particularly military ones. Two basic classes of assurance exist: vendor self assurance (through their own design, development, and testing process) and independent third party evaluations. The third party evaluations most commonly used today are the US Government TCSEC (Trusted Computer System Evaluation Criteria) and European ITSEC (Information Technology Security Evaluation Criteria). Because these processes are lengthy, on the order of multiple years to complete, they are not usually specified in commercial procurements. Often formally evaluated commercial products are obsolete before the evaluation process is finished!

**US Government Security Specifications and Levels**

With the completion of the TCSEC referenced above, the US Government defined a set of security levels products could conform to. These classes are frequently specified in Requests for Proposals, or RFPs. They are --in order of increasing security --

- Class D (Minimal if any security protection) (example: DOS, Windows)
- Class C1 (Discretionary Access Control)
- Class C2 (Discretionary Access Control and Accountability) (example: Windows NT, Trusted Mode HP-UX, MVS with RACF)
- Class B1 (Mandatory, Multilevel Access Control) (example: HP-UX 10.16, MVS with RACF)
- Classes B2, B3, A1

Of these classes, C2 is a de-facto standard for commercial secure UNIX type systems. C2 systems mediate access based upon a resource owner's discretion. That is, the owner of a resource primarily defines who on the system can access his/her information.

B1 systems are required for some government, military, and commercial applications. B1 systems support the security required to store multiple levels of classified information (e.g., confidential, secret, top secret) on a single computer system. A B1 system will prevent a user with a confidential clearance from accessing top secret documents, regardless of the top secret document owner's discretionary control. B3 and A1 systems have the same functional requirements: they represent increasing levels of assurance or trust in the implementation, reliability, integrity, and delivery of security.

**European Security Specifications and Levels**

The European ITSEC specification defines functional levels independently of assurance levels. In general, the functional levels correspond to the US Government and are designated as "F-C2, F-B1," etc. The assurance levels are in ascending order with E-1 being lowest and E-5 highest. A typical ITSEC evaluated product will have a rating of F-C2, E-3, meaning that the product has C2 functionality with an assurance rating of E-3. Commercially oriented products are usually certified to an E2 or an E3 assurance level. The discussion of ITSEC assurance requirements is outside the scope of this paper.

While European and US assurance levels really are not comparable to each other, rough approximations can be made as shown below.

### Rough Comparisons Between European and US Assurance Specifications<sup>2</sup>

	European ITSEC	US Government TCSEC
Minimal Protection	E1	D
Functional Security Testing	E2	C1 C2
	E3	C2 B1
Descriptive Top Level Specification and Verification	E4	B2 B3
Formal Top Level Specification and Verification	E5	A1

### Extensions to Security Specifications

The above specifications were originally written for monolithic mainframe-oriented systems. With the advent of client-server, networked computing, additional work was done to extend the meaning of the specifications to the new paradigm. The US Government developed the Trusted Networking Interpretation and the Trusted Database Interpretation of the TCSEC. These apply the security concepts above to networks and databases respectively. These interpretations are outside the scope of this paper.

### HP-UX 11.x Operating System Security Functionality

This section describes the security features in the general purpose, commercial HP-UX Release 11.x operating system. Only basic operating system security is discussed: kernel and UNIX commands. Systems that fall outside the scope of this presentation are:

- X-Windows and Common Desktop Environment
- Distributed Computing Environment
- Praesidium Applications and middleware
- OpenView
- Virtual Vault
- B1 special releases such as 10.09, 10.16 etc....
- Virtual Vault Operating System

### 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

<sup>2</sup> The European scheme and the US criteria look at assurance in very different ways. The mapping above is very coarse. Customers who are knowledgeable in Government security standards

standard UNIX security model to meet C2 requirements while maintaining compatibility as much as possible with legacy UNIX..

## **Standard HP-UX Security**

Standard HP-UX security follows Open Group industry standards such as UNIX95. The Standard Mode of HP-UX contains the following features.

### **Identification and Authentication**

Users are identified with an eight character maximum username. Each username is mapped in the `/etc/passwd` file to a numeric userid. A password is used for authentication. Passwords are limited to a maximum of eight significant characters, and are stored encrypted in the file `/etc/passwd`. Password aging is supported in the standard mode of the operating system. When the password expires, the user must change it at the next login. Users must be assigned membership to one or more groups. Groups are defined in the `/etc/group` file.

### **Pluggable Authentication Module (PAM)**

HP introduced the Pluggable Authentication Module (PAM) in release 11.0. This mechanism allows for multiple, replaceable authentication mechanisms in the system. For example, some users may need to be authenticated via a fingerprint reader from a third party while others only need a basic password. The PAM framework provides for this flexibility. Another example would be to require remote, dial-in users to use a Secure ID card, while users on the local network can use a password. PAM can support any of a number of authentication mechanisms such as the examples above.

### **Kerberos V5 Authentication**

User authentication in internet services such as telnet, rlogin etc. is usually achieved by sending a password over the network. These services are vulnerable against security attacks as the passwords are being sent over the network in the clear. HP introduced Secure Internet Services (SIS) in release 10.20 to prevent such attacks. SIS uses the Kerberos V5 mechanism to authenticate the user. Encrypted tickets are sent over the network instead of clear text passwords.

### **Authorization**

Root users have full authorization to administer the system, including authorization to change or defeat configured security.

Some HP-UX commands have the privilege to change their effective user id to root in order to do specific privileged functions on behalf of an unprivileged user. An example of this is the `passwd` command, which changes a user's password. These commands are called `setuid` and `setgid` commands (`suid`, `sgid` commands) and allow general users the ability to do some routine privileged functions without giving the power of root to the user.

A last component of authorization is the separation of privilege between kernel and user processes. User processes are not allowed access to each other, while the kernel has privilege to access any system resource.

### Access Control

Standard UNIX file access control is accomplished as follows. Each file has a single user and group owner. File access control is accomplished through UNIX permission bits. Permissions are read, write, execute and can be granted to the owner, group, and/or everyone. A file permission could look like:

file foo

Owner Permission rwx  
Group Permission r-x  
Other Permission ---

The owner has full access (read, write, execute). Members of the owner's group have read and execute permissions. Others have no access rights to the file foo. The owner can always change the permissions on files he/she owns. System Administrators (root users) can also change permissions on any file in the system.

Optionally HP-UX High Performance File Systems (HFS) offer access control lists which can assign the above read, write, execute permissions to an arbitrary set of users. One application of ACLs is to limit access to administrative (suid) commands to a limited set of users without giving broad root power to those users. In addition to its use to as a user tool to control file access, ACLs are also a vehicle for administrators to define administrative roles.

ACLs are not available with the Journaled File System (JFS) on any release of HP-UX 10.x or on HP-UX 11.00. JFS ACLs are included beginning with HP-UX 11.10, expected to ship during the second half of 1999.

### Audit / Accountability

Industry compatible UNIX provides for several system logs to record system activity. The primary security logs are *syslog*, *sulog*, process accounting logs, and *wtmp*. *Syslog* records basic system operations. Any application program can write logging messages to *syslog*. *Sulog* records the usage of the *su* command.

HP-UX extends upon this with the samlog which records the actions the System Administration tool (SAM) performs.

### Object Reuse

HP-UX satisfies the object reuse requirement of a secure system in the Standard mode as well as in Trusted Mode. Memory buffers and files are initialized to known values before allocation to a user to prevent a previous user's data from being disclosed.

### Assurance

HP thoroughly tests HP-UX to HP's high internal standards for product quality, reliability, and standards conformance requirements before releasing the product for customer shipment. HP monitors security advisories from CERT and FIRST responds as needed.

### Security Criteria Compliance

Standard HP-UX does not meet either the US or the European C2 security requirements. To meet these, the system must be in Trusted Mode. Trusted Mode operation is described in Section 3.3.

### Documentation

Further documentation on HP security is found on HP's Documentation Web site, <http://www.docs.hp.com>, Here can be found the HP-UX Systems Administration Tasks Manual, Managing Systems Security chapter.

## Trusted Mode (C2) Extensions to Security beyond Standard UNIX

Trusted Mode gives the administrator or security officer the following features and options not available with standard UNIX security. When the system administrator invokes trusted mode conversion through SAM, the system creates the "Protected Password Database" which provides the mechanisms and architecture to extend HP-UX security to be fully C2 Security compliant. The Protected Password Database enables:

- System Boot Authentication
- Denial of encrypted password access by non-root users
- Extending maximum password length beyond eight characters
- Forcing all passwords to conform to minimum complexity requirements
- Preventing reuse of password once they've expired
- Establishing minimum and maximum password length requirements
- Creation of a unique Audit ID for every user
- Automatic user account expiration
- Account login restrictions (time of day, day of week)
- Account disabling after a number of failed login attempts
- Login device restrictions (by tty)

Trusted Mode also has a C2-compliant auditing system which audits system activity at a low 'system call' level. The auditing subsystem is configurable so that the administrator can balance the auditing system's performance overhead with the need for user accountability. Trusted application programs can use the audit system to write their own audit records as well.

All of the above will be described in further detail in the sections below. More detailed user-oriented information can be found in the HP Document Server, HP-UX documentation, HP-UX Systems Administration Tasks found at <http://www.docs.hp.com/hpux/os/>

In addition information specific to the setup and administration of an HP-UX 10.10 or 10.20 ITSEC C2 Certified system can be found on the HP Document Server, HP-UX 10.x documentation, Administering Your HP-UX Trusted System, at [http://docs.hp.com:80/dynaweb/hpux10/inssen0a/@Generic\\_CollectionView](http://docs.hp.com:80/dynaweb/hpux10/inssen0a/@Generic_CollectionView) for 10.10 evaluated configurations and <http://docs.hp.com/hpux/content/SecUpdate1027.html> for 10.20 evaluated configurations.

### System Boot Authentication

Boot authentication provides that only authenticated and authorized users can access the system in its maintenance 'single-user' mode. This authentication is used regardless of how the system is booted: from power on or from the HP-UX command line. Boot authentication prevents unauthorized users from accessing the machine in its most vulnerable states: boot-up, initialization, and maintenance.

### Identification and Authentication

Trusted Mode provides many enhancements over Standard Mode. These enhancements give the systems administrator better control over user's access to the system as well as better security of the user account information itself.

### Encrypted Password Protection

Trusted Mode extensions provide the C2 standard compliance for protecting UNIX passwords. In particular, encrypted passwords are no longer stored in the publicly readable /etc/passwd file but are stored in the root-only readable protected password database. This makes the encrypted password unavailable to hackers/crackers who gather /etc/passwd files of encrypted passwords to attack. Passwords are much more secure in Trusted Mode than in standard UNIX.

**Long Passwords**

Password security is further enhanced by allowing longer than eight significant character passwords to be used in the system. A longer password is harder to crack than a short password.

**Password Complexity Checking**

Mandatory password complexity requirements further impedes password cracking. Password selection and generation can be enabled that:

- Allows users to generate their own password. Optional password screening can detect and reject passwords that are in a dictionary, are a login name, repeated characters, or are otherwise easy-to-guess or crack.
- Forces the system to generate a password of a combination of letters only
- Forces the system to generate a password consisting of letters, numbers, and punctuation characters
- Forces the system to generate a pronounceable phrases (based upon English)

Password security can be enabled system wide or on a per-user basis.

**Password Reuse Checking**

Password reuse checking denies a user reuse of his/her old passwords. This feature forces users to fundamentally change their passwords instead of alternating between a small number of them.

**Password Life Cycle Management**

Passwords have a life cycle (a beginning, active life, and end of life). Trusted Mode HP-UX manages each phase by setting

- A minimum time that the password must be used before it can be changed.
- An expiration time after which the user must change the password or the account will be locked. Only the root (superuser) can unlock the account.
- A warning time that asks the user to change the password prior to expiration

**Login Controls**

The system administrator can establish per user controls on when that user can access the system. These controls fall into two categories: time-based and device-based access controls.

- Time-Based Controls, the user's access is regulated by the time of day and day of week.
- Device based access controls, the system administrator can dedicate specific mux or DTC ports for a user. If a user tries to login via an unauthorized port, he/she is denied access to the system.
- Account locking after consecutive failed login attempts. If a hacker tries to login into an account and fails after a configurable number of consecutive attempts, then the account is locked. This prevents hackers from continually trying to break into an account if they don't have a valid password.

**Audit / Accountability**

Trusted mode enhances standard UNIX system logging with the low level system call audit function. Using the Audit ID extension of Trusted Mode to uniquely identify users, the audit system can be configured to audit any of over 100 security relevant system calls on a per-user basis.

System call auditing is the most secure form of accountability. It is also the most resource intensive, consuming CPU cycles and disk space. By carefully selecting the system calls which are audited, the system administrator can optimize and balance the audit data gathered with the system performance cost of gathering it. HP provides a tool through the System Administrator Manager (SAM), to view the audit records. This tool can be configured to filter out audit records that are of no interest to the system administrator.

As the operating system grows from release to release, so does the number of security relevant, auditable system calls. The System Administrator must ensure that the calls audited are checked and meet the Administrator's security objective with every system upgrade.

#### **Assurance, Formal Certification to Standards**

All releases of HP-UX 11.x are TCSEC and ITSEC C2-compliant. HP-UX 10.10 and 10.20, when in Trusted Mode, were formally evaluated and certified to ITSEC Functionality Class C2, Assurance Class E3.

The formally certified Operating Systems are certified in a limited configuration consisting of the base kernel and commands only. Networking, the X11 Windowing system, and SAM all are outside the formally certified system configuration. These operating system components, of course, are interoperable with Trusted Mode: they simply were not part of the formally evaluated system.

#### **Trusted Mode Interoperability with other Applications**

Because Trusted Mode has some HP proprietary extensions to the relatively unsecure industry-standard definition of UNIX, occasionally applications that interact directly with the standard UNIX security APIs or data structures will not work with Trusted Mode HP-UX. Applications or development tools which use the available Trusted Mode APIs are interoperable with no modifications. Applications that do not access user accounts, passwords, etc. are interoperable with no modifications.

#### **HP-UX Security Manageability**

Operating system security by necessity is oriented towards protecting the single host system. As Administrators have many systems to manage at a time, however, managing each system individually becomes prohibitive. As a result several management tools are available to help the administrator set up, configure, and modify networks of their systems' security configuration. Of these, NIS (Network Information Service or Yellow-Pages) and NIS+ are available as part of the standard HP-UX product. Administration of HP-UX security can be managed with these tools as described below.

#### **System Administrator (SAM)**

SAM is the basic administration for configuring a single HP-UX system. Through SAM, the administrator converts the system to Trusted Mode and from there administers all the user configuration and audit configuration for the system.

SAM can be configured to restrict what its authorized users can do. Called Restricted SAM, this feature allows the root administrator to delegate limited authority to others without giving the entire power of root away. For example through Restricted SAM a user account administrator role could be implemented. With Restricted SAM a single administrator has only limited power, thereby increasing security.

#### **NIS**

NIS was developed by Sun Microsystems as a method to centrally configure and manage groups of UNIX systems. One NIS Master server can manage all the user accounts and standard security configuration of an entire domain of NIS Clients in a network. The standard mode of HP-UX security can be managed with NIS. Trusted Mode security (extended passwords, auditing, etc.) cannot be supported in an NIS domain.

#### **NIS+**

NIS+ is the second generation of NIS and supports extended security attributes. With the introduction of NIS+ in HP-UX 11.00, Trusted Mode security can be supported and centrally managed via an HP-UX NIS+ Master. This master can centrally manage security attributes of Standard Mode HP-UX, Trusted Mode HP-UX, and third party vendor NIS+ clients.

**Cryptographic APIs**

HP-UX 11.0 supports the Common Data Security Architecture. This architecture, developed at Intel Corporation and standardized through the Open Group, provides an industry standard API into a Public Key Infrastructure. Beginning in June, 1999 HP-UX 11.0 customers have access to CDSA version 1.2 along with an X.509v3 Certificate Library and the most commonly used cryptography algorithms.

CDSA is delivered initially as a separate, add-on product to HP-UX 11.0, J4262AA. The cryptography algorithms (available separately, at no charge) are available in three versions, specific to the customer's particular export-control jurisdiction. These versions are:

Product J4261AA Worldwide Importable cryptography for customers who are limited by their government to cryptography strength of 40 bits.

Product J4250AA Worldwide Exortable cryptography for customers who are not limited by their government, but who are limited by US Export controls. This product has cryptography strength of 56 bits.

Product J4260AA North America Only cryptography, which is export restricted to US and Canadian customers. Customers outside of the US and Canada require a specific export license in order for HP to provide this cryptography.

All the cryptography modules above are available as a no-charge download from HP's software web site, [www.software.hp.com](http://www.software.hp.com).

Further details and specifications of the CDSA subsystem are in Appendix A of this White Paper.

## HP-UX Security Feature Summary

The above features provide system administrators and end users core security needed to reliably protect their data and machine resources. HP-11.00 security features and benefits are summarized below.

Feature	Mode S = Standard Mode, T = Trusted Mode	Benefit
Industry Standard UNIX Security	S	Known, standard security feature set that is easily administered across multiple UNIX platforms.
HFS Access Control Lists	S, T	Delegation of read, write, execute access permissions to any group of users
Restricted SAM	S, T	Allows users other than root to have limited administration privileges.
Large (>60000 User Ids)	S, T	Allows larger numbers of users to be allowed access to the system.
NIS Manageability NIS+ Manageability	S	Central management of standard UNIX security for a network of multivendor UNIX systems.
Pluggable Authentication Module	S, T	<ul style="list-style-type: none"> <li>Multiple authentication mechanisms</li> <li>Strong authentication beyond passwords</li> <li>Framework for new authentication schemes</li> </ul>
System Boot Authentication	T	Allows only authenticated, authorized users to access the system in single-user mode.
Encrypted Password Protection	T	Hides encrypted passwords from password crackers
Long Passwords	T	Makes passwords more difficult to crack than standard 8 character passwords.
Password Complexity Checking	T	Makes passwords more difficult to crack by forcing them to be unrecognizable words, phrases etc. that would be found in a dictionary.
Password Reuse Checking	T	Makes passwords more difficult to crack by forcing users to create different passwords every time their password expires. Prevents users from alternating their passwords.
Password Life Cycle Management	T	Minimized chance that passwords will be compromised.
Kerberos V5 Authentication	S, T	Allows remote users to be authenticated without sending clear text passwords over the network
Login Controls	T	Prevents suspicious access during off-hours or from remote locations
Auditing	T	Secure, fine-grained record of user activity that can be used to identify system misuse.
Common Data Security Architecture with Cryptography library	S, T	Industry standard cryptographic API approved around the world for use by any application. Included are widely used cryptographic

<b>Feature</b>	<b>Mode</b> S = Standard Mode, T = Trusted Mode	<b>Benefit</b>
(6/99)		algorithms.
C2 Security Compliance	T	Compliance to a specification that is widely regarded as a baseline for commercial host system security.
NIS+ Manageability	T	Allows central management of a group of Trusted Mode systems on a network through the recently enhanced NIS+ framework
ITSEC Certification	T	Independent third party review and examination of security. Improves customer confidence in evaluated product. (HP-UX 10.10 and 10.20 only)

Further information can be found on HP's Document Server as described above.

#### Field Support and Patches

Security escalations are given the highest priority to resolve in the Lab. HP works with the major computer security centers FIRST, CERT, AUSCERT, etc. to communicate security defects and their resolution. Visit the following web sites to get more information: <http://www.cert.org> and <http://www.first.org>.

To subscribe to automatically receive future NEW HP Security Bulletins from the HP Electronic Support Center via electronic mail, do the following:

Find the HP Electronic Support Center page at:

<http://us-support.external.hp.com> (for US, Canada, Asia-Pacific, and Latin-America)

<http://europe-support.external.hp.com> (for Europe)

Click on the Technical Knowledge Database, register as a user (remember to save the User ID assigned to you, and your password), and it will connect to a HP Search Technical Knowledge DB page. Near the bottom is a hyperlink to the HP Security Bulletin archive. Once in the archive there is another link to the current security patch matrix. Updated daily, this matrix is categorized by platform/OS release, and by bulletin topic.

## Feature Comparison by HP-UX Release

Below is a comparison of security features by release.

### Standard Mode HP-UX Security Feature Availability

	10.01	10.10	10.20	11.00
Industry Standard UNIX Security	x	x	x	x
Object Reuse	x	x	x	x
HFS Access Control Lists	x	x	x	x
Restricted SAM	x	x	x	x
Large (>60,000) User IDs			x	x
Keberos V5 Authentication			x	x
NIS Manageability	x	x	x	x
Pluggable Authentication Module				x
NIS+ Manageability				x
JFS Access Control Lists				
CDSA Cryptographic API and Cryptography				x <sup>1</sup>

### Trusted Mode HP-UX Feature Availability (Includes all the Standard Mode Features and the Following)

	10.01	10.10	10.20	11.00
Encrypted Password Protection	x	x	x	x
Boot Authentication	x	x	x	x
Long Passwords	x	x	x	x
Password Complexity Checking	x	x	x	x
Password Reuse Checking				x <sup>2</sup>
Password Life Cycle Management	x	x	x	x
Login Controls	x	x	x	x
Auditing	x	x	x	x
C2 Security Compliance	x	x	x	x
JFS Support in Trusted Mode			x	x
NIS+ Manageability				x
ITSEC Certification		x	x	

1. CDSA is provided as an add-on product J4262AA CDSA International available June, 1999
2. Password reuse checking was delivered as part of Extension pack 9804.

## References

Further information can be found at the sources below.

### Trusted Computer Systems Evaluation Criteria

US Government Publication that describes the Security levels commonly used: C2, B1, etc. Also known as the "Orange Book."

### Security Survival

A source book from The Open Group to help administrators make UNIX systems secure. The Open Group can be contacted at [www.opengroup.org](http://www.opengroup.org). The book is published by Prentice Hall, ISBN 0-13-266628-6.

### X-Open Baseline Security Specification

An Open Group Specification that gives good guidance on how to configure a secure system. More information about this specification is available from The Open Group on the web at [www.opengroup.org](http://www.opengroup.org).

### Practical UNIX and Internet Security

Simpson Garfinkel and Gene Spafford, Purdue University. This book is a common reference system administrators and security professionals rely upon. A description of the book can be found at <http://www.ora.com/catalog/puis/noframes.html>

### Web Security and Commerce

Simpson Garfinkel and Gene Spafford, Purdue University. A description of the book can be found at <http://www.ora.com/catalog/websec/noframes.html>

### Systems Administration Tasks Manual

This HP 9000 manual provides system administrators the basic concepts and procedures for configuring security. The manual can be found online from the HP Document Server, HP-UX documentation, HP-UX Systems Administration Tasks found at <http://www.docs.hp.com/hpux/os/>

### Administering Your HP-UX Trusted System

This HP 9000 manual provides system administrators the necessary information to set up, configure, and maintain an evaluated C2 level Trusted System. There are two manuals which can be found online at [http://docs.hp.com:80/dynaweb/hpux10/inssen0a/@Generic\\_CollectionView](http://docs.hp.com:80/dynaweb/hpux10/inssen0a/@Generic_CollectionView) describes 10.10

<http://docs.hp.com/hpux/content/SecUpdate1027.html> describes 10.20

### Praesidium Program Web Site

The Praesidium security web site is <http://www.hp.com/go/security>

### Versecure Web Site

The Versecure (formerly International Cryptography Framework) web site for more information on HP's encryption program is <http://www.hp.com/go/versecure>

### HP Electronic Support Center

<http://us-support.external.hp.com> (for US, Canada, Asia-Pacific, & Latin-America)

<http://europe-support.external.hp.com> (for Europe)

### Trusted Mode Application Compatibility White Paper

Written as an internal HP document, this white paper describes what application developers need to be aware of in making their products compatible with HP's proprietary Trusted Mode security extensions. This paper can be found at:

[http://runner.cup.hp.com/~projects/security/projects/ISU\\_WhitePaper.asc](http://runner.cup.hp.com/~projects/security/projects/ISU_WhitePaper.asc)

Please ask your HP representative for a copy of this paper.

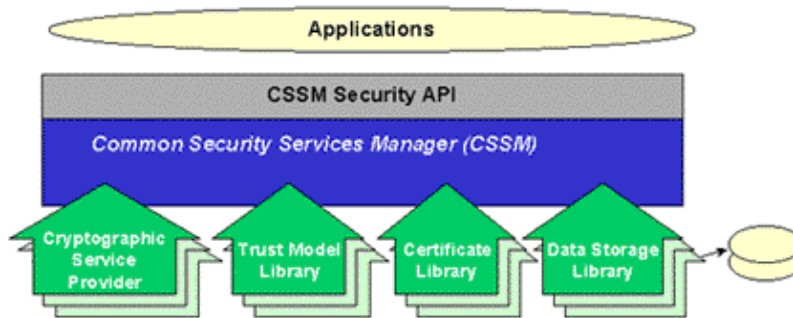
## Appendix A: CDSA Cryptography Specifications and Availability

This appendix describes in more detail the specifications of the Common Data Security Architecture (CDSA) and cryptography provided in DART 45 (June 1, 1999 Ship Release Date) and HP-UX 11.10. Availability of the cryptography is dependent upon international import and export regulation, which may change from time to time. CDSA provides a shared library, which any application written to HP-UX CDSA may use. There are no restrictions on the use of CDSA or its supported cryptography: any application written to the CSSM Security API may use any of the cryptography provided. CDSA and the cryptography are provided at no additional charge and are supported as part of the HP-UX operating system.

DART 45 provides CDSA and the Cryptography as separate products supported on HP-UX 11.0. HP-UX 11.10 includes CDSA within the OS itself. All CSPs are delivered as separate products available as free downloads from [www.software.hp.com](http://www.software.hp.com).

### CDSA Overview

CDSA originally was developed by the Intel Corporation as a general purpose interface to a Public Key Infrastructure. CDSA provides structured interfaces as shown below:



CDSA version 2.0 has been ratified by the Open Group as an Industry Standard. Because CDSA version 2.0 is not yet available for general release, HP-UX supports contains a predecessor version, CDSA version 1.2. While CDSA 1.2 is not the industry standard release, it is the release HP and other major software suppliers have converged upon for initial product introductions. As CDSA v2.0 becomes available, HP plans to incorporate it into subsequent HP-UX releases.

CDSA has a modular architecture, with each module performing specific functions. The CSSM Security API provides applications a common, stable, defined interface designed to be used by attaching to lower-level "plug in" service provider libraries. Service providers perform four separate functions:

- The Cryptographic Service Provider (CSP) contains encryption algorithms used by the applications.
- The Trust Model Library (TML) provides a means to define the "chain of trust." The TML defines how Public Key Certificates are trusted and how trust can be passed through a PKI Certificate chain.
- The Certificate Library (CL) provides the function of parsing public key certificates. Usually these will be X.509 certificates, although nothing in the CDSA architecture or standard prohibits other PKI certificate formats.
- The Data Storage Library (DSL) provides the mechanism to store and retrieve certificates.

To support HP-UX 11.0, CDSA is available as a separate, free product downloadable from [www.software.hp.com](http://www.software.hp.com) as HP product number

J4262AA CDSA International SW/LTU

Beginning with the HP-UX 11.10 release, CDSA will be included with the operating system itself. There are no US export restrictions on these product.

Whether downloaded as a separate product or used as part of HP-UX 11.10, the CDSA system contains the CSSM API, the Common Security Services Manager and a Certificate Library plug in. Cryptographic Service Provider Plug-ins are available separately as described in the following section. Trust Model libraries and Data Storage Libraries are not provided in this release as they were felt to be application specific; that is, application developers would want to specify or provide these modules themselves.

### **Cryptographic Service Provider**

HP provides the Cryptographic Service Provider (CSP) as part of the CDSA solution. The CSP is subject to worldwide import, export, and useage restrictions on encryption. HP is making available three versions of the CSP, one of which will be suitable for every country in which HP does business. These versions are:

**North America Only:** This version is restricted to North American customers. This version may not be exported from the United States or Canada without an export license.

HP may request a license for specific customers or applications that require strong encryption and have US Commerce Department approval. Contact the HP Sales Representative or HP Export Administration for procedures on how to request an export license for the North America Only version of the CSP.

This version of the CSP is available from <http://www.software.hp.com> as part number

J4260AA CSP US/CAN 128 Bit-DES SW/LTU

**Worldwide Exportable from the US:** This version has US Commerce Department approval for export to any country except the "terrorist 7."

The Worldwide Exportable version of the CSP is freely exportable from the United States; however, some countries have controls that preclude its import. IT IS THE CUSTOMERS' RESPONSIBILITY TO COMPLY WITH LOCAL LAWS REGARDING THE IMPORTATION OF THIS CSP.

This version of the CSP is available from <http://www.software.hp.com> as part number

J4259AA CSP 56 Bit-DES SW/LTU.

**Worldwide Importable:** This version provides weaker encryption than the Wordwide Exportable version and is, thus, freely exportable from the United States. There are no known import controls on the strength of cryptography , making this version universally importable into any country HP does business. IT IS THE CUSTOMERS' RESPONSIBILITY TO COMPLY WITH ANY LOCAL LAWS REGARDNG THE IMPORTATION OF THIS CSP.

The Worldwide Importable version of the CSP is from <http://www.software.hp.com> as part number

J4261AA CSP 40 Bit SW/LTU

**Cryptographic Functions Provided in Each Version of the CSP**

	<b>Worldwide Importable</b>	<b>Worldwide Exportable</b>	<b>North America Only</b>
<b>56 Bit DES</b>	N/a	Available	Available
<b>CDMF DES</b>	Available	Available	Available
<b>Triple DES</b>	N/a	N/a	Available
<b>RC2</b>	Limited to 40b key	Limited to 56b key	2048
<b>RC4</b>	Limited to 40b key	Limited to 56b key	2048
<b>RSA Public Key Cryptosystem</b>	Limited to 512b for encryption Supports 768, 1024 bit keys for signatures	Limited to 512b for encryption Supports 768, 1024 bit keys for signatures	2048b max key size for encryption and signatures
<b>Diffie-Hellman Key Exchange</b>	Limited to 512b keys	Limited to 512b keys	2048b max key size
<b>SHA-1, HMAC SHA-1</b>	Available	Available	Available
<b>MD5, HMAC MD5</b>	Available	Available	Available
<b>Digital Signature Algorithm</b>	1024 bit max key size	1024b max key size	2048 bit max key size
<b>OAEP</b>	Available	Available	Available
<b>PRNG</b>	Available	Available	Available

**Certificate Library (CL)**

The Certificate Library supports the parsing of X.509v3 Public Key Certificates. Specific X.509v3 fields supported are:

- X.509 Version ID (1, 2, or 3)
- Serial Number (arbitrary but should be unique for each Certificate Authority)
- Signature Algorithm ID (example: RSA with MD5)
- Issuer Distinguished Name (the CA that issued the certificate)
- Start Validity Date
- End Validity Date
- Subject Distinguished Name
- Public Key Algorithm ID (example: RSA)
- Signature
- Extensions (Optional)

Certificates may have various classifications, and increasingly, developers are including more information inside a certificate through optional extensions. The CL supports self-signed certificates required as a root for a Certificate Authority.

The Certificate library also supports creation and parsing of X.509v2 Certificate Revocation Lists, used to revoke previously issued X.509 certificates.

**Worldwide Import/Export Control Considerations**

CDSA v1.2 is freely exportable from the United States. There are no known import controls on the API. Likewise the Certificate Library falls outside the scope of any international controls and is freely importable and

exportable. Data Storage Libraries and Trust Model Libraries, too, are outside of the scope of controls. CSPs are export controlled as previously described.

The worldwide import/export considerations about cryptography and cryptographic APIs have been evolving over the last several years. Further evolution is expected. The information in this White Paper is accurate as of the time of the initial HP-UX CDSA product release. Contact your HP Sales Representative or HP Export Administration for current information or details specific to particular circumstances.

### **Availability**

As previously discussed, the CDSA product is available in two components: CDSA/CSSM and the CSP appropriate for the end user's particular jurisdiction.

#### **Availability of CDSA/CSSM**

The CDSA / CSSM application interface and Certificate Library are available in two ways:

HP-UX 11.0 customers must download from HP's software server <http://www.software.hp.com> the product

J4262AA CDSA International SW/LTU

CDSA/CSSM will be included with HP-UX 11.10. No further download is necessary.

#### **Availability of the CSPs**

The three different versions of the CSP, the North America Only, Worldwide Exportable, and Worldwide Importable are available as free downloads from HP's software server (<http://www.software.hp.com>) to those customers who request are eligible for them. IT IS THE CUSTOMER'S RESPONSIBILITY TO ENSURE HE/SHE IS COMPLYING WITH LOCAL LAWS REGARDING THE IMPORTATION OF THIS CSP.

Customers who do not have internet access may request copies of the software from their HP sales representatives.

### **Conclusion**

By providing the Common Data Security Architecture (CDSA) on HP-UX, HP has enabled application developers to write security-dependent applications with confidence that the cryptography will be available on all end user systems. Customers around the world have access to the strongest security allowed by law at no additional charge.

### **Applicable Reference Documents and Standards**

CDSA version 2.0 specification is available from The Open Group at <http://www.opengroup.org/security/cdsa/index.htm>

CDSA version 1.2 specification is available at [http://www.intel.com/ial/security/specs\\_1\\_2.htm](http://www.intel.com/ial/security/specs_1_2.htm)

Hewlett Packard has a white paper outlining the use of CDSA on HP-UX, [Common Data Security Architecture \(CDSA\) White Paper](#), which is included with the release of CDSA at /usr/share/docs/cdsa.ps. It is also available on the HP document server at <http://www.docs.hp.com>

DES is specified in FIPS 46-2 and ANSI 3.92-1981. Modes of operation are specified in FIPS 81 and ANSI 3.106.

CDMF is the subject of US Patent 5,323,464.

RC2 is specified by draft-rivest-rc2desc-00.txt.

Diffie-Hellman is specified in PKCS#3, IEEE P1363, and ANSI X9.42 draft standards

DSA is specified in FIPS 186 and ANSI X9.30 (part 1).

RSA is specified in PKCS #1

MD5 is specified in RFC 1321.

SHA-1 is specified in FIPS 180-1 and ANSI X9.30 (part 2).

HMAC in general is specified in RFC 2104. HMAC-MD5 is specified in RFC 2085.

OAEP is specified in Section 13.3 of the April, 1998 draft of IEEE P1363 standard.

Random number generation uses SHA-1 in accordance with FIPS 186 Appendix 3.