Software Product Description

PRODUCT NAME: DEC MLS+ For Trusted Display Stations, Version 3.1A **SPD 61.23.00**

DESCRIPTION

DEC MLS+ Version 3.1A, for Trusted Display Stations, is Digital Equipment Corporation's security-enhanced implementation of DEC OSF/1® V2.0 software specifically designed for Alpha based Display Station use. The MLS+ Trusted Display Station provides client support only.

The DEC MLS+ operating system is designed to meet the B1/CMW level of security specified in the following documents:

- Department of Defense, National Computer Security Center. Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).

- Security Requirements for System High and Compartmented Mode Workstations (DDS-2600-5502-87).

The DEC MLS+ operating system is a trusted version of the 64-bit advanced kernel architecture based on Carnegie Mellon University's Mach V2.5 kernel DEC OSF/1 design with components from Berkeley Software Distribution 4.3 (BSD), 4.4 BSD, UNIX System V, and other sources.

In addition, to ensure a high level of compatibility with ULTRIX MLS+, the DEC MLS+ Version 3.1A operating system is compatible with Berkeley 4.3 and System V programming interfaces.

The trusted implementation of the X Window System is based on the industry standard OSF/Motif® V1.2.2 window manager and the X11 R5 window server.

DEC MLS+, Version 3.1A, is based upon the DEC OSF/1 Version 2.0 and includes many extensions and security enhancements.

SECURITY ENHANCEMENTS

The DEC MLS+ system provides protected processing of sensitive information. The heart of the system is the Trusted Computing Base (TCB), a set of protection mechanisms that enforce the system's security policy. Security features are transparent to applications, with the exception of security policy violations.

Console Password

The DEC MLS+ system includes password protection at the boot-ROM level. When the console password feature is enabled, a user must correctly enter a password before executing privileged console commands. For example, a user must know this password to boot an image other than that specified by the default bootpath.

Access Policies

The DEC MLS+ system security policy includes the following access policies:

- Discretionary Access Control (DAC) - provides both the traditional UNIX mechanism of "owner, group, and other" access permissions and a more granular access control list (ACL) mechanism, controlled by the object's owner.

- Mandatory Access Control (MAC) - provides a mechanism for the security officer to define sensitivity labels that can be applied to all processes and security-related objects (such as files, sockets, and windows) in the system.

- Information Labels (ILs) - provides a mechanism for the user to more finely reflect the sensitivity of the actual contents of information in a system object. When information is added to a file (object) or process (subject), the system automatically adjusts the information label as necessary.

The DEC MLS+ system security policy extends to both the window system and the Network File System, providing a consistent security policy across the entire system.

Trusted X Window System

The MLS+ trusted implementation of the X Window System has the following features: discretionary access control (DAC), mandatory access control (MAC), information labels (ILs), auditing, object reuse and trusted path. All windows and icons are properly labeled by a trusted implementation of Motif Window Manager. Interwindow data moves (cut and paste) are monitored by the Trusted Selection Handler. The trusted path region is controlled by the Trusted Path Handler. All trusted clients are monitored for proper operation by a Trusted Client Handler.

The MLS+ Security Policy, implemented at the protocol level of X11, allows well-behaved, ICCCM-compliant X clients to run off-the-shelf on an MLS+ system. The Trusted X Window System is based on Version 11 Release 5 of X Windows and OSF/Motif Version 1.2.2.

The X server's default visual is dynamic (PseudoColor) and it supports a multilevel security policy.

Trusted MultiSIX Networking

MLS+ has a number of trusted network facilities. DEC MultiSIX is the name of the comprehensive trusted network strategy implemented by MLS+.

The Trusted Network (TNET) architecture supports the BSD 4.3 and 4.4 socket mechanism and the Internet Protocol Suite. TNET lets an MLS+ host establish TCP/IP connections to both MLS+ and non-MLS+ hosts, using extensions to the socket mechanism to pass security attributes (such as sensitivity labels) between MLS+ hosts. When communicating with non-MLS+ hosts, security attributes are removed from exported messages and added to imported messages.

TSIX 1.0 (RE) Session Attribute Modulation Protocol (SAMP) transports security attributes between endpoints of a network connection. For more information, refer to the Standards section in this SPD.

Trusted networking facilities include FTP, remote commands, NFS ®, NIS, and TELNET:

- Trusted File Transfer Program (FTP) - Provides most of the standard FTP server capabilities while preserving the MLS+ mandatory and discretionary access policies. An FTP connection is established by using the MLS+ client's sensitivity label as the connection sensitivity label. Files that are transferred during this session contain the sensitivity label. The file information label is propagated to the file using the normal information label float rules.

- Trusted rlogin, rsh, rcp Commands - Enforces MLS+ security policies. Unprivileged users can use these commands to connect to remote MLS+ systems on a network.

- Trusted Network File System (NFS) - Provides the ability to mount both labeled (trusted) and unlabeled (standard) file systems. For a labeled file system mounted between MLS+ hosts, trusted NFS maintains the correct security attributes for each remote-mounted file. For an unlabeled file system, an administrator assigns security attributes to the mount point; these attributes are applied on all files in the mounted file system.

- Trusted TELNET - Supports a trusted TELNET server, which provides the TELNET server capabilities while preserving the MLS+ mandatory and discretionary access policies. A TELNET connection is established using the MLS+ client sensitivity label as the connection sensitivity label.

- Trusted Network Information Services (NIS) - Provides a distributed data lookup service for sharing information between systems on a network and allows users to update their NIS passwords from an NIS DEC MLS+ V3.1A client.

TCP/IP Support
MLS+ allows for TCP/IP network communications over supported network devices. The TCP/IP protocol suite is implemented in the socket framework.

FDDI Support
MLS+ provides FDDI fiber optic support. Please refer to the OPTIONAL HARDWARE section for specific hardware supported.

Trusted Interprocess Communications (IPC)
MLS+ provides sockets that are based on the Berkeley UNIX operating system structure. This support provides a framework for I/O over a network.

The DEC MLS+ system provides socket modifications that support the passing of security attributes across AF_UNIX and AF_INET connections. AF_UNIX sockets are local and have access to the full set of security attributes available to the local system. AF_INET sockets pass the security attributes associated with the process at either end, but must rely on the TNET databases for information about the amount of trust vested in a remote host.

Sockets support the following security attributes: sensitivity labels, information labels, privilege set, login user ID (LUID), effective user ID (EUID), effective group ID (EGID), supplementary groups, and process ID.

Unlabeled Hosts
For MLS+ systems to interoperate with systems that do not have MultiSIX support (unmodified hosts), MLS+ provides the ability to define security attributes for non-MLS+ systems. MLS+ can interoperate with any system that supports the standard TCP/IP and TCP/UDP protocol family. The unmodified host is treated as a single-level host. Unmodified host support also allows an MLS+ host to act as the gateway between a single-level LAN and a multilevel LAN.

Multilevel Security Directories
Multilevel Security (MLS) directories provide a solution to the problem of managing files and directories at different sensitivity labels. This allows unprivileged users to place files at different sensitivity levels in the same directory.

Hidden Directories
For compatibility purposes, the MLS+ system supports the “hidden” directories used by some vendors of compartmented mode workstations.

Separate Administrative Roles
The system provides for four separate administrative roles as an alternative to the traditional "root" account. MLS+ provides a simple-to-use interface for these four functions:

- Information System Security Officer (ISSO) - Responsible for security aspects of system management:
  - — Assigns privileges and authorizations to users, programs, and processes, thus controlling the ability of any user to perform a specific action.
  - — Maintains and assigns proper information and sensitivity labels.
  - — Collects and reviews audit data.
  - — Assures that system objects are properly protected.
- System Administrator - Responsible for general system management and account creation. The system administrator is also responsible for granting authorizations to the ISSO.
- Operator - Responsible for day-to-day operations.
- Network Information System Security Officer (Net ISSO) - Responsible for adding and removing hosts and maintaining their security attributes.

STANDARDS

TSIX(RE) 1.0 Trusted Networking
The DEC MLS+ system offers secure networking based on the security protocols from the Trusted System Interoperability Group (TSIG), which has published its version of the TSIX(RE) 1.0 specifications. MLS+ utilizes the TSIX(RE) 1.0 of a network connection. The Security Attribute Token Mapping Protocol is used to translate security attributes to a network representation common between two or more hosts.

RFC 1108
MLS+ has the ability to generate IP Security Options according to Internet RFC 1108. This allows mandatory access controls to be used at the network level.

SHARED LIBRARIES

MLS+ provides a full complement of dynamic shared libraries, based on System V semantics, which increase system performance, reduce minimum hardware requirements, and ease system management.

USER ENVIRONMENT

Shells
DEC MLS+ provides the following shells:

- C Shell
- Bourne Shell from System V
- Korn Shell

All shells are programmable and allow for a tailorable user environment.

Dynamic Loader
DEC MLS+ uses a SVR4 compatible loader to load shared libraries dynamically.

This loader provides the following enhanced features:

- Calling into dynamically loaded shared libraries
- SVR4 symbol resolution semantics, including symbol preemption
- Prelinking of libraries for fast program loading

The COFF object file format is supported for all forms of object files.

File System Support
The base DEC OSF/1 file system architecture is based on OSF/1 VFS, which is based on the Berkeley 4.3 Reno Virtual File System (VFS). VFS provides an abstract layer interface into files regardless of the file systems in which the file resides.

DEC MLS+ supports many of the file system types supported by DEC OSF/1, including:

- UNIX File Systems (UFS) - based on the Berkeley Fast File system
- Network File System NFS)
- Memory File System (MFS)
- ISO 9660 Compact Disc File System (CDFS)
- File-on-file Mounting File System (FFM)
- /proc File System

Multilevel Security (MLS) Directories
The MLS directories are the default directories (the ones made by mkdir). MLS directories provide the following:

- Both files and filenames have sensitivity labels (SLs) and information labels (ILs). A directory has a sensitivity label but no discrete information label. The information label of a process that is reading directory entries floats to the high-water mark of the information labels for the directory entries being read.

- A directory can contain files at different sensitivity levels. Each directory has a minimum SL. The sensitivity of both the filename and the file must dominate the sensitivity label of the directory. A directory can contain filenames whose SLs range from the directory's minimum SL up to System High.

- Processes with different sensitivity labels can create temporary files the same way they would in a nonsecure UNIX implementation, as a unique name with a common pathname prefix (/tmp or /usr/tmp). An unprivileged process sees only filenames whose sensitivity labels are dominated by the sensitivity label of the process.

Common Access Method (CAM)
Common Access Method is an ANSI standard for the software drivers that provide the interface between an operating system and a SCSI device. The CAM implementation in MLS+ is compatible with ANSI X3.131-1986, Level 2 and supports SCSI-2 based CAM.

Graphics Support
DEC MLS+ includes the Trusted DECwindows Motif graphical user interface. DECwindows incorporates the OSF/Motif user interface as the design center for the DECwindows applications. As such, the Motif user interface defines a powerful model for interacting with the MLS+ Operating System by using a point-and-click metaphor.

Based on the X Window System, Version 11, Release 5, and OSF/Motif R1.2.2, DECwindows Motif supports the following X Window System standards:

- X11 protocol
- Base set of workstation fonts
- Xlib programming library
- X Toolkit Intrinsics library
- X Server

A license for Motif and for the X Window System is included with DEC MLS+.

SYSTEM MANAGEMENT

Installation

DEC MLS+ is classified as Customer Installable. Installation Services are available for those customers who desire installation of the software product by an experienced Digital Software Specialist.

Support Tools

MLS+ provides a Verifier and Exercisor Tool (VET) which contains a set of system exercisers and an online diagnostic monitor.

HARDWARE REQUIREMENTS

The DEC MLS+ Operating System can execute on supported Digital Alpha systems and must include the minimum system configuration as described in the SUPPORTED HARDWARE section. The actual amount of work supported at one time, with good performance, depends on the types of processing performed as well as on the physical memory and secondary storage available.

- MLS+ requires the minimum component of main memory to be 32 MB, although 64 MB is recommended for better performance.
- MLS+ requires a system disk capable of holding the supported software subsets. The DEC MLS+ Trusted Display Station requires a minimum of 600MB disk.
- MLS+ supports the backup devices listed in the OPTIONAL HARDWARE section.
- The supported load devices include: CD-ROM (RRD42 or RRD43) and Network.
- MLS+ requires one Digital graphics display console for Alpha systems.

OPTIONAL HARDWARE

Additional memory and/or secondary storage may be required depending upon the need for MLS+ software or optional software products and usage of the MLS+ operating system.

Note

Combinations of hardware options are subject to limitations such as bandwidth, physical configuration restraints, thermal dissipation, and electrical loads/power.

System configuration details are described in the Systems and Options Catalog.

Hardware options that are supported by the MLS+ operating system are listed in the SUPPORTED HARDWARE section. All device drivers for these hardware units contained in MLS+ are warranted by Digital.

OPTIONAL SOFTWARE

DEC Open3D Version 2.2 for DEC OSF/1 provides support for PXG, ZLXM1, ZLXM2, and ZLXM3 graphics accelerators on Alpha workstations running the DEC MLS+ Operating System, plus an extensive set of programming libraries for use by developers of new applications. Refer to SPD 45.07.xx for further information.

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIUM

CD-ROM

ORDERING INFORMATION

The MLS+ operating system license provides a licensed user the right to use the software as described within this Software Product Description.

Prerequisite Licenses

A license for DEC OSF/1, either as part of a packaged systems or ordered separately, is a prerequisite for DEC MLS+.

DEC OSF/1 Operating System License

QL-MT4A*-** - Software 2 User Base Licenses

DEC MLS+ Operating System Licenses

QL-511AE-BC - DEC MLS+ U/A 2 User License for Display Stations

MEDIA AND DOCUMENTATION

The MLS+ Software Media kit includes a CD-ROM that contains the operating system binaries, complete MLS+ on-line documentation, DEC OSF/1 documents as Bookreader files, hardcopy Release Notes and Installation Instructions.

QL-0UNAA-H8	DEC MLS+ CD Kit - includes DEC MLS+ V3.1A on one CD-ROM, hardcopy Release Notes & Installation Instructions.

The full Software Documentation kit includes hardcopy versions of the documentation found on line via the CD-ROM, excluding the references pages, and additional documentation that is published by companies other than Digital Equipment Corporation. The full Software Documentation kit is a complete hardcopy documentation set for MLS+.

Documentation published by companies other than Digital Equipment Corporation is not available on line and is only available through the Software Documentation kit.

The following hardcopy documentation is available separately:

QA-0UNAA-GZ	DEC MLS+ Full Documentation Kit contains all end user, programmer, and system documentation except reference pages, which are online or available in a separate hardcopy kit
QA-0UNAB-GZ	DEC MLS+ Startup Documentation Kit - Includes Release Notes and Installation Instructions.

QA-0UNAC-GZ	DEC MLS+ V3.1 End-User Documentation Kit - Includes Concepts and Features Guide, User's Guide and Reader's Guide & Index
QA-0UNAD-GZ	DEC MLS+ V3.1 Administrator/Programmer Kit - Includes Programming Guide, Trusted Networking Guide, and Label Encodings

DEC MLS+ SOFTWARE PRODUCT SERVICES

QT-511A*-**	Software Product Services for DEC MLS+ As a prerequisite, DEC OSF/ Software Product Services are required: QT-MT4A*-**

A variety of service options are available from Digital. For more information, contact your local Digital office.
* Denotes variant fields. For additional information on available licenses, services, and media, refer to the appropriate price book.

SOFTWARE LICENSING

The DEC MLS+ operating system software is furnished under the licensing of Digital Equipment Corporation's Standard Terms and Conditions.

DEC MLS+ requires the DEC OSF/1 base system base license and the appropriate interactive use licenses. See the DEC OSF/1 SPD for more information.

LICENSE MANAGEMENT FACILITY SUPPORT

DEC MLS+ supports Digital's License Management Facility (LMF). The LMF provides on-line checking of software licenses and enables easier software management.

If a base license is not registered and activated using the License Management Facility, then only login by root is permitted for system management purposes.

For more information about Digital's licensing terms and policies, contact your Digital account representative.

SOFTWARE WARRANTY

Warranty for this software product is provided by Digital with the purchase of a license for the product as defined in the applicable Digital Standard Terms and Conditions.

DEC MLS+ SUBSET SUPPORT

This Display Station Software only supports the following subsets:

MLSBASE310	Base System (-Required-)
MLSBIN310	Standard Kernel Objects (Kernel Build Environment)
MLSBINCOM310	Kernel Header and Common Files (Kernel Build Environment)
MLSCLINET310	Basic Networking Services (Network-Server/Communications)
MLSCMPLRS310	Compiler Back End (Software Development)
MLSDPSFONT310	Adobe Fonts (Windowing Environment)
MLSFONT15310	DECwindows 100dpi Fonts (Windowing Environment)
MLSHWBASE310	Base System - Hardware Support (-Required-)
MLSHWBIN310	Hardware Kernel Objects (Kernel Build Environment)
MLSHWBINCOM310	Hardware kernel Header and Common Files (Kernel Build Environment)
MLSMITFONT310	X Fonts (Windowing Environment)
MLSNFS310	NFS™ Utilities (Network-Server/Communications)
MLSSER310	X Servers (Windowing Environment)

MLSTRX310	Trusted Worksystem Software (-Required-)
MLSX11310	Basic X Environment (Windowing Environment)
MLSINET310	Additional Networking Services (Network-Server/Communications)
MLSFONT310	DECwindows 75dpi Fonts (Windowing Environment)

All other subsets are unsupported in this configuration.

SUPPORTED HARDWARE

The following table lists supported hardware for MLS+. Combinations of hardware options are subject to limitations such as bandwidth, physical configuration constraints, and electrical load and power supply.

The content of this hardware configuration section is intended to specify the device limitations and provide a general guide. It does not describe all possible hardware configurations or circumstances. Any particular configuration should be discussed with Digital. Contact Digital for the most up-to-date information on possible hardware configurations.

Digital reserves the right to change the number and type of devices supported by MLS+. The minimum hardware requirements for future versions and updates of MLS+ may be different from current hardware requirements. For configuration details about Alpha systems, refer to the Digital Systems and Options Catalog and the Networks and Communications Buyer's Guide.

Table 1 AlphaStation 200 4/100, 4/166, 4/233; AlphaStation 250 4/266; AlphaStation 400 4/233

CD-ROM Drive:	RRD42	RRD43	
Disks:	RZ25L RZ26L RZ28B	RZ26 RZ28	
Diskettes:	RX23		
Adapters:	KZPAA (PCI SCSI 2)		
Network Adapters:	DEFPA (PCI FDDI)	DE434, 435, 436, 450 (PCI Ethernet)	
Monitors:	VRC15 VRT17	VRC16	VRC21
Keyboard:	PCXAL-XX	LK411	
Graphics:	PB2GA-FA (ATI Mach 64 CX)[1]	PBXGA (ZLXp-E series)	

[1]Supported on 100 Model only.

Note: This product includes software developed by the University of California, Berkeley and its contributors.