Product Standard

Operating System and Languages:

COE Platform Security

The Open Group

Product Standard

Operating System and Languages: COE Platform Security

Document Number: X02CR

Published in the U.K. by The Open Group, May 2003.

Any comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza
Forbury Road
Reading
Berkshire, RG1 1AX
United Kingdom

or by Electronic Mail to:

OGSpecs@opengroup.org

Product Standard

NAME

COE Platform Security

LABEL FOR LOGO

No label.

DESCRIPTION

The COE Platform Security Product Standard identifies security-related criteria for COE Platform compliance. Service, agency, and system-unique requirements are outside the scope of this document, as are the overall security requirements of systems built using the COE.

COE Platform security features and capabilities, as identified in this Product Standard, are grouped into the following categories:

- Identification and Authentication (I&A)
- Security Audit
- Service Availability
- Discretionary Access Control
- Markings
- Object Reuse
- Data Confidentiality
- System Integrity
- System Architecture
- Trusted Facility Management
- Other Requirements

CONFORMANCE REQUIREMENTS

A COE Platform implementation shall meet the requirements in the COE Security Software Requirements Specification (SSRS).[1]

[1] Technical Standard, May 2003, COE Security Software Requirements Specification (SSRS) (ISBN: 1-931624-31-3, C035), published by The Open Group.

The following general requirements shall also apply:

- The system shall have the operating system security modules enabled and shall adhere to the COE Security Features Developer's Guide specifications.
- All command-line modes and/or features shall require user authentication. This authentication shall require a password.
- The system shall not provide files or directories with universal write access.
- The system shall provide a unique COE Group ID (GID), and document it in the COE Platform Conformance Statement.
- The system shall establish an appropriate *umask* value, and document it in the COE Platform Conformance Statement.
- The system shall not provide any set-user-ID root or set-group-ID *appropriate-value* (the group ID for the root user) shell scripts unless documented in the COE Platform Conformance Statement together with a reference to an approved Problem Report.
- The system shall not place any temporary files in the system-maintained temporary directory that are sensitive to alteration, deletion, or disclosure to unauthorized users.
- The system shall not create files that are sensitive to alteration or deletion by unauthorized users in any directory where such unauthorized users have write access, and shall not have write permissions set for such unauthorized users.
- The system shall not create files that are sensitive to disclosure to unauthorized users in any directory where unauthorized users have read access.
- The system shall provide that entry to and exit from the command line mode causes an entry into the system audit logs that specifies the date, time, and user involved.

OPERATIONAL ENVIRONMENT

Not applicable.

PORTABILITY ENVIRONMENT

Not applicable.

OVERRIDING STANDARDS

Not applicable.

INDICATORS OF COMPLIANCE

The following are the required Indicators of Compliance:

- A report from the Automated Security Test Suite

MIGRATION

Not applicable.