

IEEE Standards Interpretation for IEEE Std 1003.1™-1990 IEEE Standard for Information Technology--Portable Operating System Interfaces (POSIX®)

Copyright © 2001 by the Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue New York, New York 10016-5997 USA All Rights Reserved.

Interpretations are issued to explain and clarify the intent of a standard and do not constitute an alteration to the original standard. In addition, interpretations are not intended to supply consulting information. Permission is hereby granted to download and print one copy of this document. Individuals seeking permission to reproduce and/or distribute this document in its entirety or portions of this document must contact the IEEE Standards Department for the appropriate license. Use of the information contained in this document is at your own risk.

IEEE Standards Department Copyrights and Permissions 445 Hoes Lane, Piscataway, New Jersey 08855-1331, USA

Interpretation Request #60

Topic: real UID, effective UID and saved-set UID **Relevant Sections:** 2.2.2.4, 5.6.4.2

Does an implementation that possesses the constraint such that: The process's real UID, effective UID, and saved-set-UID are the same for every process of a login session and cannot be changed by POSIX.1 function calls. conform to POSIX.1-1990.

When both POSIX.1 conformance and `_POSIX_SAVED_IDS` defined in `<unistd.h>` (`{_POSIX_SAVED_IDS}` support) are required, does an implementation that possesses the constraint such that: The process's real UID, effective UID, and saved-set-UID are the same for every process of a login session and cannot be changed by POSIX.1 function calls. conform.

In the rationale for this interpretation, please address the question. "When a profile of the POSIX.1 standard requires feature 'A', does this implicitly specify the requirement of all other features needed to support the required feature 'A'?" (In other words, which takes precedence, the specification of feature 'A' or the failure to specify one of the other features needed to support feature 'A'?)

Interpretation Response

An implementation where the real UID, effective UID, and saved set-user-ID of the process are constrained to be the same for every process of a login session and cannot be changed by POSIX.1 function calls does conform to IEEE Std 1003.1-1990 (POSIX.1-1990) if it meets the rest of the requirements for the standard. If a process has the same value for its real UID, effective UID, and saved set-user-ID, it must have the appropriate privilege in order to use `setuid()` to change its real and effective user IDs. The description of appropriate privileges (2.2.2.4) says "There may be zero or more such means". A conforming implementation need not provide a means to associate with

a process the appropriate privilege to change user IDs.

The description of the `chmod()` function says, in part (5.6.4.2): Additional implementation-defined restrictions may cause the `S_ISUID` and `S_ISGID` bits in 'mode' to be ignored.

This means that a conforming implementation need not provide a means by which the `S_ISUID` bit can be set for a file, so the `exec` type functions might not be able to change a process's effective user ID.

There is no requirement in POSIX.1-1990 that would require that an implementation provide a means to change user IDs other than those that are explicitly specified in POSIX.1-1990.

Implications for IEEE Std 2003.1-1992: Assertions 13 and 14 of 5.6.1.2, which test the semantics of `exec` type functions for files with the `S_ISUID` and `S_ISGID` masks set, should be changed to show that they are subject to the `PCTS_CHMOD_SET_IDS` testing constraint (see 1.4.5.1 of IEEE Std 2003.1-1992):

13(PCTS_CHMOD_SET_IDS?A:UNTESTED)

14(PCTS_CHMOD_SET_IDS?A:UNTESTED)

Until these assertions can be modified, there will be a conflict between IEEE Std 1003.1-1990 and IEEE Std 2003.1-1992. Test suite implementors and test suite users will have to make the choice whether to test for conformance to 1003.1-1990 or to 2003.1-1992.

Background information on impact on 2003.1-1992: The "constraint":

The process's real UID, effective UID, and saved-set-UID are the same for every process of a login session and cannot be changed by POSIX.1 function calls, was unknown, when IEEE Std 2003.1-1992 was produced and balloted. I also assume this was unknown to ISO/IEC 9945-1:1990. This "constraint" requires additional changes to 2003.1 than those listed above to adequately specify the allowed behavior. Since this feature requires the IDs to be the same for every process of a login session, they cannot change. Therefore, changes are also required for `setuid()` and `setgid()` in POSIX.1 and POSIX.3.1.

Question 2 Response

IEEE Std 1003.1-1990 does not define any semantics for `{_POSIX_SAVED_IDS}` that can be detected by an application running on an implementation on which each process's real UID, effective UID, and saved set-user-ID are the same and cannot be changed, as long as the implementation meets all of the requirements of the standard.

On such an implementation there is no way that a conforming application can tell whether saved set-user-IDS are implemented or not. The behavior of a conforming application cannot be affected by whether `{_POSIX_SAVED_IDS}` is defined or not. Thus, such an implementation would be conforming.

The Standard is silent on the issue of whether it is appropriate to define `{_POSIX_SAVED_IDS}` on a system on which the user IDs of a process cannot be changed. This means that it is unspecified whether it is appropriate, so it is conforming to set the constant or not to set it.

The rationale for the definition of 'unspecified' (B.2.2.1, page 198, lines 547-549) expresses the intent of the 1003.1 working group on issues of this sort: There is a natural tendency to infer that if the standard is silent, a behavior is prohibited. That is not the intent. Silence is intended to be equivalent to the term 'unspecified'.

Rationale for Interpretation

It is not the intent of IEEE Std 1003.1-1990 to create implementation requirements that go beyond the explicit specifications in the Standard. In particular, it is not intended that there be implicit linkages between the various choices that IEEE Std 1003.1-1990 leaves open for the implementor, only the linkages explicitly stated in the Standard.

Profiles are beyond the scope of IEEE Std 1003.1-1990, and it is the responsibility of the author of a profile to ensure that the specifications in the profile are sufficiently precise that they will have the desired effect in light of the implementation choices that are allowed by IEEE Std 1003.1-1990. The author of a profile is free to explicitly restrict the implementor's choices in any way that is compatible with IEEE Std 1003.1-1990. The author should take care to understand the explicit provisions of IEEE Std 1003.1-1990, and to make explicit any special requirements that are not spelled out there.

If specific features are needed, the profile should ask for them. IEEE Std 1003.1-1990 does not define a hierarchy of prerequisites that requires that one optional feature be supported because a related feature is required.