IEEE P1003.0 Draft 13 – September 1991

Copyright © 1991 by the
Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, NY 10017, USA
All rights reserved as an unpublished work.

This is an unapproved and unpublished IEEE Standards Draft, subject to change. The publication, distribution, or copying of this draft, as well as all derivative works based on this draft, is expressly prohibited except as set forth below.

Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only, and subject to the restrictions contained herein.

Permission is hereby also granted for member bodies and technical committees of ISO and IEC to reproduce this document for purposes of developing a national position, subject to the restrictions contained herein.

Permission is hereby also granted to the preceding entities to make limited copies of this document in an electronic form only for the stated activities.

The following restrictions apply to reproducing or transmitting the document in any form: 1) all copies or portions thereof must identify the document's IEEE project number and draft number, and must be accompanied by this entire notice in a prominent location; 2) no portion of this document may be redistributed in any modified or abridged form without the prior approval of the IEEE Standards Department.

Other entities seeking permission to reproduce this document, or any portion thereof, for standardization or other activities, must contact the IEEE Standards Department for the appropriate license.

Use of information contained in this unapproved draft is at your own risk.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA
+1 (908) 562-3800
+1 (908) 562-1571 [FAX]

rules with the character set.

— Presentation rules: the application platform should have the ability of providing fallback presentation rules for the presentation of coded characters that have no associated graphic shape.

(3) Character set identifier: the application platform should provide the ability to uniquely identify each coded character set to allow compatibility checks and translation or transliteration to and from other registered character sets. This ensures data integrity in the communication of data across computers and networks.

(4) Character set selection: the application platform should allow the end-user or the application to select the coded character set to be used; otherwise, the application must automatically select a default coded character set according to preset parameters. It must be possible to switch to other coded character sets and to invoke translation routines where required.

Editor's Note: From here to the end of 5.1, the term ''[operating] system'' has been replaced numerous times with ''application platform'', without further diff marks. D

(5) Data announcement: the application platform could benefit from having the ability to recognize the coded character set of data entities (files, messages, etc.). One way of doing this is to store the character set identifier together with the data; standardization efforts are under way to formalize this process, with consideration being given to the level of granularity of such identification (e.g. file, word, character). The announcement enables the application to prohibit updates with data coded in other character sets, thus ensuring data integrity even in distributed systems.

(6) Data presentation: the application platform should be able to present data on different display or output devices, potentially according to rules in a repository, including escapement of characters and selection of different shapes. Preparing data for presentation may involve extensive translation and transliteration due to potential hardware limitations of the printers and displays used in a particular installation.

(7) Data communication: the application platform should be able to transmit and receive data from communication systems and to maintain the integrity of the information. In an internationalized environment, this capability might include data translation due to different coded character sets being used by different service categories of the application platform.

(8) Data input: the ability to enter data is not necessarily controlled by the application platform. The complexity of the input of Asian languages though might strongly support the idea of a standardized input mechanism interface. Depending on how other internationalization service requirements are met, it might also be beneficial for input data to carry some form of character set identification.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.1.4.1.2 Cultural Conventions

Besides using different characters and different languages, countries throughout the world have also developed quite different cultural conventions. Even within one country we can find significantly different cultural environments. The prime example is Switzerland, where French, German, Italian, and Rhaeto Romanic are officially accepted languages. Combined with the language preferences are conventions about the formats of time, date, numeric values, and measuring systems. Currency symbols, paper formats, hyphenation, and collating are dependent on cultural conventions. End-user-oriented applications have to address these issues to provide a familiar local view, which helps to prevent operating errors.

The general service requirements for cultural conventions are:

(1) Cultural convention repository: The application platform must have the ability to store and access rules and conventions for cultural entities. These might be areas with a common language, geographic areas, or areas with common cultural or historic background. The repository should contain specifications and presentation rules for:

— Date and time formats: indicating the formats associated with the particular cultural entity. For example, while in the US the date is expressed in the format month/day/year, the European preferred format is year-month-day for data processing purposes and day-month-year in personal use. Japan counts the years according to the reign of the current emperor. Additionally, twenty-four-hour clocks, which are prevalent in Europe, are commonly used only in military circles in the US, while the terms ‘‘am’’and ‘‘pm’’,denoting morning and afternoon, are used by the general public. These are only a few examples for the cultural differences in this area. The application platform must be able to store the preferred forms for date and time for a specific cultural entity and make it available upon request in this format.

— Week and day numbering: in Europe, the week starts on Monday, in the US on Sunday. The application platform should be able to supply D
the requesting program with the needed information, potentially from D
a repository according to specified rules.

— Formats of numeric fields: handling of numeric fields in unfamiliar formats is one of the major reasons for human errors. The application platform must provide the service to format the values according to specifications in the repository. The characters that signify the decimal point (comma, period, etc.) must be defined, as well as the number of decimals, the grouping of digits before the decimal point and the presentation of negative values.

— Currency symbols and field length: the handling of currency symbols in the different cultural areas must be provided by the general internationalization services. The currency symbols might be more than one digit long and can appear before or after the currency field. The format of currency fields might differ from that of numeric fields; for

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

example, in Portugal the $-sign is used as the decimal point. Information about these conventions must be stored in the repository and be used by the application platform for local formatting of currency fields. Not necessarily a service, but similarly important, is the understanding, that due to the value of different currencies, the field lengths must be considered carefully. Also some currencies do not have decimals (e.g., Italian Lira).

D

— Paper formats: internationally usable and portable applications must be able to print on different paper formats. While quart format is predominant in the US and the far east, the DIN standardized A-formats are used in Europe. Printer drivers must be able to adjust their output to local formats, defined in the cultural convention repository.

(2) Cultural repository selection: these repositories must be available to all applications. Users and applications must be able to select a repository from the application platform; a default value must be provided if no selection is made. An additional service allows dynamic switching to other repositories upon user or program requests.

(3) Collating rules: besides the generic binary and character-set-dependent sorting rules, the application platform must have the ability to sort data according to local rules, defined in the repository. An example for culture-dependent collating rules is the handling of umlauts; while they are sorted with the base characters in Austria, they are sorted at the end of the alphabet in Sweden. Adding complexity, they can be sorted differently within one country between normal business use, such as dictionaries, and in telephone books. Other idiosyncrasies are the sorting of one character as two (the German ‘‘sharp-s’’ sorts as ‘‘sz’’in Austria and ‘‘ss’’in Germany), or two characters as one (the Spanish ‘‘ch’’sorts as one character), or the position of accented characters in a string, and more. User-defined collating tables in the cultural convention repository allow culture or application-dependent sorting services.

5.1.4.1.3 Natural Language Support

The POSIX OSE must give users the ability to select a natural language for their dialogue with the system and applications. While it is unrealistic to expect all application platforms to support all possible natural languages, error messages, online documentation and help facilities, selection menus, and the relevant user interaction with these services must be prepared for translation into the supported user-selectable natural language. Additionally, the POSIX OSE must support differences between the natural language selected by the user for interaction with the application platform and that selected for use within a particular application. For word- and text-processing, the service includes hyphenation and spell checking with possible thesaurus support in different languages. The problem is complicated by the fact that data can contain text in different languages in the same document.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

The service requirements for natural language support are:

(1) Multilingual capability: the application platform should be able to support more than one language simultaneously. For example, one process might be providing French language capabilities while another process operated in Japanese. The application platform must be able to let users select their preferred languages for communication with the application and allow them to switch dynamically to another language. The application platform must also have the capability to assign a default language, based on parameters for the application platform, the specific workstation, the user identification, or the application.

(2) Natural language message system: the application platform must have the capability to present (display, print, ...) messages, menus, forms, and online documentation in the language, selected by the user. The application platform must be able to support multiple languages simultaneously for different users and it must allow the user to switch from one language to another. The following problems must also be handled correctly:

— The program code of the application should be able to be independent from any particular natural language, presenting messages in the natural language used within the internationalized user environment selected by the user.

— Variable message length: the application platform should support the presentation of messages of variable length, as translation into other languages changes the length of the message; English text is usually quite short compared to the same text in, e.g., German or Finnish. Ample room must be available in the display field to accommodate this variation.

— Inserted parameters and word order: the application platform should have the capability of inserting variable parameters into messages at the location appropriate for the user selected natural language.

(3) Support of local keyboards: the application platform must be able to correctly interpret the input from keyboards that have been modified locally to support the local character sets.

(4) Local language user interaction: the application must be able to accept solicited input from the user in the language selected by the user, without dependence within the application logic on a particular natural language or set of cultural conventions. For example, many applications use the first characters of prompts to make selections; this method is not acceptable in an internationalized system. The translation process changes the prompts and with them their first character; more than one prompt could have the same start-character and the program logic would not work. Multiple languages must be supported simultaneously.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

D

5.1.4.2 API Service Requirements D

All the general services defined in 5.1.4.1 must be accessible from the applications through requests to the application program interface. The API service requirements can be structured in the same way as the general requirements, which they call for. D D D D

5.1.4.2.1 Cultural Conventions

— Cultural convention invocation: the application platform must allow the application to invoke a specific cultural convention from the repository. It must automatically invoke the default convention set, if no selection is made by the application.

— Cultural convention change: when requested by the application or the user, the application platform must change the used cultural convention dynamically.

— Provide local values: upon request from the application, the application platform must return local formats for time, date, calendar, numeric fields, currency fields and symbols. D

— Local sort and comparison: when requested by the application, the application platform must compare and sort data according to the local collating rules defined in the cultural convention repository.

5.1.4.2.2 Natural Language Support

— Language selection: the application platform must present messages, menus, forms, online documentation, and user interaction in the natural language selected by the user or automatically by the system based on preset parameters for the application, the session, the user, or the system.

— Change of language: upon request from the user, the application platform should be able to dynamically change, prior to the invocation of a particular user application, the language used for messages, menus, forms, online documentation, and user interactions. D D D

5.1.4.3 Localization Tools Requirements

Internationalization of application platforms and applications is the basis for their localization in the different countries. It is important for the user that this localization can be performed in a well prepared, organized way without the need to know the internal structure of the application platform or the application. The following requirements for localization tools are key to successful localization of application platforms and applications:

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

406 — Character set repository tools: tools should be provided to set up and main- D
407 tain character set repositories. They must also allow the addition of new
408 character sets to the repository.

409 — Cultural convention repository tools: tools should be provided to set up and D
410 maintain the cultural convention repositories. Addition of new cultural
411 environments must be possible. User-definable collation tables are essen-
412 tial parts of these repositories; tools to define and maintain them must be
413 offered.

414 — Translation support tools: facilities for the set-up and maintenance of local
415 language message files, menus, forms, online documentation, and user D
416 interaction tables should be provided. The addition of new supported D
417 languages should be allowed by such tools. Additionally, any such transla- D
418 tion tools should allow revision control, so that only new or changed text D
419 would require translation for new software releases. D

420 5.1.5 Performance and Capacity Values

421 The POSIX OSE provides a foundation for implementations of application plat-
422 forms to support multiple cultural conventions. It is expected that the specific
423 sets of supported cultural conventions will be implementation defined. While
424 ideally localization should not impact the performance of applications or applica-
425 tion platforms, extensive character set translation and complex sorting operations
426 might impact the performance of localized systems.

427 The application platform must allow the implementation of as many cultural con-
428 ventions and character sets as are necessary to accommodate the different market
429 environments in which it will be used.

430 5.1.6 Standards, Specifications, and Gaps

431 There are not many standards available that deal with internationalization. The
432 majority of current standards describe character sets, both for control characters
433 and for graphic characters in different coding schemes (7-bit, 8-bit, etc.). A few
434 standards address the formats of time and date, and some standards touch peri-
435 pherally on the subject of data announcement.

436 An example of how cultural conventions and languages are currently supported is
437 the *locale* () function. It allows the application developer to select portions or all of
438 predefined support features for national languages and local cultural conventions.
439 The portions, called categories, correspond to the areas of functionality; presently
440 supported are LC_CTYPE , LC_COLLATE , LC_TIME , LC_MONETARY , and
441 LC_NUMERIC. Other categories, like message handling, are likely to be imple-
442 mented, too. Other systems have started to implement similar philosophies of
443 general services to support local cultural conventions.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

444 #### 5.1.6.1 Current Standards in the POSIX OSE

445 ##### 5.1.6.1.1 International Standards

446 — ISO 646: 1983, *ISO 7-Bit Coded Character Set for Information Interchange*

447 Defines the binary representation of 128 control, (Latin) alphabet, digit,
448 and symbol characters. Describes in general the use of the control charac-
449 ters. Describes option of national replacement characters.

450 — ISO 2014: 1976, *Writing of Calendar Dates in All-numeric Form*

451 This international standard specifies the writing of dates of the Gregorian
452 calendar in all-numeric form, signified by the elements year, month, and
453 day.

454 — ISO 2022: 1986, *ISO 7-Bit and 8-Bit Coded Character Sets—Code Extension*
455 *Techniques*

456 Defines techniques for expanding the number of characters represented by
457 the base character set.

458 — ISO 3307: 1975, *Representation of Time of the Day*

459 This international standard is designed to establish uniform time represen-
460 tation based upon the 24-hour timekeeping system. It provides a means for
461 representing local time of the day and Universal Time in digital form for
462 the purpose of interchanging information among data systems.

463 — ISO 4031: 1987, *Representation of Local Time Differentials*

464 This international standard specifies a standard means for representing
465 local time differentials to facilitate interchange of data among data sys-
466 tems.

467 — ISO 4217: 1987, *Codes for the Representation of Currencies and Funds*

468 Specifies the representation of currencies and currency symbols

469 — ISO 4873: 1986, *ISO 8-Bit Code for Information Interchange—Structure and*
470 *Rules for Implementation*

471 Outlines the structure of the ISO 8-bit code and rules for implementation.

472 — ISO 6093: 1985, *Presentation of Numerical Values in Character Strings for*
473 *Information Interchange*

474 Specifies three presentations of numerical values, which are represented in
475 character strings in a form readable by machine, for use in interchange
476 between data processing systems. Also provides guidance for developers of
477 programming languages standards and Implementor's of programming pro-
478 ducts. These representations are recognizable by humans, and thus may be
479 useful in communication between humans.

480 — ISO 6429: 1988, *ISO 7-Bit and 8-Bit Coded Character Sets—Control Func-*
481 *tions for Coded Character Sets*

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Defines control functions and their coded representations for use in a 7-bit code, an extended 7-bit code, an 8-bit code, or an extended 8-bit code. Specifies a C0 set, a C1 set, control functions derived there from, and a number of independent control functions.

— ISO 6936: 1988, *Conversion between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. (ITA) 2*

Specifies the rules for conversion between ITA 2 representation of 58 characters and the ISO 646 representation of 128 characters.

— ISO 6937-1: 1983, *Coded Character Sets for Text Communication—Part 1: General Introduction*

Defines terms and concepts used in describing and using code representations of character sets.

— ISO 6937-2: 1983, *Coded Character Sets for Text Communication—Part 2: Latin Alphabetic and Non-alphabetic Graphic Characters*

Defines a repertoire of Latin alphabetic and non-alphabetic characters. Specifies binary representation of the characters. Specifies rules for the definition and use of character sets that are subsets of the repertoire.

— ISO 7350: 1984, *Registration of Graphic Character Subrepertoires*

Specifies the procedures for preparing, registering, publishing, and maintaining the register of graphic character sets that are composed from the character repertoire of ISO 6937 and the procedures for assigning identifiers to the sets.

— ISO 8601: 1988, *Representation of Dates and Times*

Specifies the representation of dates A.D. in the Gregorian calendar and times and representation of periods of times. Applicable whenever dates and times are included in information interchange.

— ISO 8859-x: 1987, *8-Bit Single-Byte Coded Graphic Character Sets*

Specifies a set of up to 191 graphic characters by means of a single 8- bit byte. The versions (‘‘-x’’) indicate different coded character sets:

-1 Latin Alphabet No. 1

-2 Latin Alphabet No. 2

-3 Latin Alphabet No. 3

-4 Latin Alphabet No. 4

-5 Latin/Cyrillic Alphabet

-6 Latin/Arabic Alphabet

-7 Latin Greek Alphabet

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

519 -8 Latin/Hebrew Alphabet

520 — CCITT T.61, 1985: *Character Repertoire and Coded Character Sets for the*
521 *International Teletex Service*

522 Describes detailed definitions of the repertoires of graphic characters and
523 control functions to be used in the international Teletex service. The
524 means by which supplementary character repertoires are defined are also
525 described.

526 **5.1.6.1.2 Regional Standards**

527 Presently, no regional internationalization standards which relate to the scope of
528 this guide have been adopted.

529 **5.1.6.1.3 National Standards**

530 Many of the international ISO standards have ''twins'' in the national standards
531 bodies; i.e., the same text is given a local standard identification. Also, national
532 standards bodies have often developed standards for local representation of time,
533 date, and currency. The implementation of these standards into an international-
534 ized system is a prime example of localization.

535 Here are some standards that have no international equivalent:

536 — GB 2312: 1980, Chinese national character set standard

537 — JIS X 0208: 1983, Japanese national character set standard

538 — KS C 5601: 1987, Korean national character set standard

539 **5.1.6.2 Emerging Standards in the POSIX OSE**

540 **5.1.6.2.1 International Standards**

541 The rapid development of business opportunities in the Pan-European and the
542 Asian market has spawned a wealth of activities to develop standards for the sup-
543 port of internationalization in the field of information technology. These emerg-
544 ing standards deal with character sets, language neutral user interfaces, and
545 communication.

546 — ISO DIS 10646: *Multiple Octet Coded Character Set*

547 This standard will permit the presentation of all of the world's scripts in
548 computer based systems, and their unambiguous interchange between one
549 system or person and another. It is applicable to the representation, pro-
550 cessing, storage and presentation of the written form of the languages of
551 the world.

552 — ISO/IEC DIS 10367: *Repertoire of Standardized Coded Graphic Character*
553 *Sets for Use in 8-Bit Codes*

554 This standard specifies a unique graphic character set for use as G0 set and
555 a series of coded graphic character sets of up to 96 characters for use as the

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

G1, G2, and G3 sets in versions of ISO 4873. All sets specified in this standard are shown as elements of an 8-bit code.

— ISO/IEC CD 9995-x: *Information Technology—Keyboard Layouts for Text and Office Systems*

This family of standards defines the layout of keyboards so that they can be used for input of multilingual information.

5.1.6.2.2 Regional Standards

The European Community is in the process to define European standards, called EN (Europaeische Norm). No internationalization standards have yet been adopted. To be supplied

5.1.6.2.3 National Standards

National standards under development which relate to internationalization include:

— CSA-Z243.200-88: *Canadian National Keyboard Standard for the English and French Languages in Text and Office Systems*

5.1.6.3 Gaps in Available Standards

5.1.6.3.1 Standards and Specifications Outside the POSIX OSE

The PC character set was defined at a time, when the international standards for single-byte, 8-bit character sets were not available yet. Therefore, the PC character set was accepted and still is a de facto standard in the PC world. The concept of different code pages has been implemented in MS-DOS and WINDOWS-3 is using ISO 8859-1 internally for compatibility reasons with other systems. Some companies have gone similar routes and developed their own, multilingual character sets for specific applications, the general trend is clearly towards ISO standards wherever they exist.

A consortium of software and hardware companies is developing ''Unicode,'' a 16-bit character set standard for worldwide use.

5.1.6.3.2 Unsatisfied

While the character set arena is heavily populated, very little work is done in other areas of internationalization of products. Standards should be developed for:

— Cultural conventions repository

— Application program interface services for cultural conventions

— Application program interface services for character set handling

— Multilingual collating rules

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

591 — Input methods interface for Asian languages

592 — Standards for message delivery systems

593 — Data announcement standards

594 Additionally, no standards currently exist that support the following character set D
595 and data representation functionality: D

596 (1) Character set invocation: the application platform must allow the appli- D
597 cation to invoke a specific character set from the character set repository. D
598 It must automatically invoke the default character set, if no selection is D
599 made by the application. D

600 (2) Character set changes: When requested by the application, the character D
601 set must be changed dynamically. D

602 (3) Character set identifier: the application program must be able to write D
603 the character set identifier to data and must be able to retrieve the D
604 identifier for requested data. D

605 (4) Character set identifier comparison: the application platform must, upon D
606 request from the application or automatically, compare the character set D
607 identifiers of interacting data in the application (input, processing, data D
608 storage, communication, and output). D

609 (5) Character set translation: the application platform must provide transla- D
610 tion of character sets, when requested by the application or automati- D
611 cally, when detecting a mismatch in the comparison process. D

612 ### 5.1.7 OSE Cross-Category Services

613 Not applicable.

614 ### 5.1.8 Related Standards

615 The nature of internationalization as being a cross-component facility is that it
616 affects just about every element in the information processing world. Thus,
617 almost all standards in this environment are related to the subject. Here we will
618 point out a few major families of standards, strongly related to internationaliza-
619 tion.

620 — ISO DIS 8613: Office Document Architecture and Interchange Format
621 (ODA)

622 This family of standards, ODA/ODIF, consist of:

623 1.2 Introduction and General Principles

624 2.2 Document Structures

625 3 Document Processing Reference Model

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

626 4.2 Document Profile

627 5.2 Office Document Interchange Format

628 6.2 Character Content Architectures

629 7 Raster Graphics Content Architectures

630 8 Geometric Graphics Content Architectures

631 — ISO 8824: 1987, *Specification of Abstract Syntax Notation One ASN. 1*

632 Specifies a notation for the definition of abstract syntaxes, enabling Appli-
633 cation Layer standards to define the types of information they need to
634 transfer using the Presentation service. It also specifies a notation for the
635 specification of values of a defined type.

636 — ISO 8825: 1987, *Specification of Basic Encoding Rules for Abstract Syntax*
637 *Notation One (ASN. 1)*

638 Defines a set of encoding rules that can be applied to values of types
639 defined using the notation specified in ASN. 1. Application of these encoding
640 rules produce a transfer syntax for such values. It is implicit in the
641 specification of these encoding rules that they are also be used for decoding.

642 — All programming language standards, since programming languages have
643 to support internationalization, and have to work correctly in localized
644 environments. Their generated code itself has to work ‘‘localized.’’

645 **5.1.9 Open Issues**

646 See 5.1.6.3.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.2 System Security Services D

Responsibility: Michelle Aden D

HLJ : This is a complete clause replacement for Draft 13. It is not further diff-marked to avoid clutter. D D

5.2.1 Overview and Rationale

Information is the key to successful use of a system. For example, if used effectively and efficiently, information may be used to underpin enhanced service and to aid the derivation of strategic plans. Much of this information, for example, personal customer details and business financial plans, will be of a sensitive nature.

Although authorized users may be able to take advantage of the POSIX Open System Environment (OSE) to increase productivity and efficiency, unauthorized individuals may also be able to take advantage of the OSE to steal, manipulate or to deny others access to information held within the system, or to deny involvement in some transaction performed via the system.

Security services must therefore be provided within the system if it is to prevent these unauthorized activities. To achieve an optimum degree of confidence in the correctness and effectiveness of a system's security services, a system specific security policy must be derived and appropriate security functionality designed into the system at the beginning of its life cycle.

A relatively high degree of protection for ordinary computer systems can be achieved if system administrators correctly configure and maintain the system according to recommended security guidelines and practice, such as those described within the *X/Open Security Guide* {*ref*}. However, additional security facilities must be supported within the system to achieve protection against the small percentage of attackers who are noncasual, and who are determined to breach the security of the system. It is the intent of the security extensions to the base POSIX interface standard to support these additional security facilities.

The four basic security objectives of a system are to maintain:

— Confidentiality. The system must prevent unauthorized viewing of data.

— Integrity. The system must prevent unauthorized alteration or deletion of data.

— Availability. The system must ensure that authorized users are not prevented from accessing and processing data.

— Accountability. The system must ensure that users are made accountable for their actions, for example to ensure that users are correctly billed for system usage.

Different user groups may place different emphases upon these four basic security objectives. For example, the military security sector may place more importance upon confidentiality than accountability while, correspondingly, the commercial

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

sector may place more importance upon accountability than confidentiality.

5.2.2 Scope

One of the goals of system security is to provide defense in depth, such that if one layer of security is breached then further layers of security will limit and/or prevent unauthorized activities within the system.

To achieve a high degree of confidence in the correctness and effectiveness of the security of a system that will be processing sensitive information, security must be designed into the system at the beginning of its life cycle.

A System Security Policy (SSP) defines what it means for a specific system to be ''secure'' and, as such, forms the basic security input into the system lifecycle. Specification of an SSP is therefore axiomatic to the design of a secure system.

Although the SSP defines what security measures will be provided within the system, it is the system design documentation that defines how these security measures will actually be implemented.

One aspect of an SSP may be that it mandates conformance with the POSIX security extensions.

The IEEE POSIX security group (P1003.6) has responsibility for defining the security extensions to the base POSIX interface standard. The POSIX security interface specifications are intended to assist in the construction of a secure system. They do not, in isolation, provide any protection against threats to a system.

5.2.3 Reference Model

The POSIX Reference Model partitions the Application Program Interface and the External Environment Interface into a collection of services, each one of which may have a security component. These individual components may operate independently or cooperatively with other security components. For example, a user identification and authentication operation may include elements of the User Interface Services, Communication Services, and Database Services.

5.2.4 Service Requirements

Through an analysis of the potential threats and requirements of the system, the system security objectives and hence the necessary System Security Policy (SSP) rules may be derived. This analysis must also take into account appropriate corporate, legal, and standardization requirements.

System confidentiality, integrity, availability, and accountability may be supported by the following security objectives:

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

721 **Technical Security Objectives**

722 — Identification And Authentication. A system entity, such as a user or sys-
723 tem element, must prove that its claimed identity is legitimate, such that
724 another system entity may place confidence in that claimed identity.

725 — Access Control. Access to system resources will be restricted to authorized
726 entities only. Residual data contained within an object will be securely
727 erased before it may be reused by a system entity.

728 — Accountability And Audit. System users must be made accountable for
729 their actions. Audit trails of these actions will then be maintained and util-
730 ized such that unauthorized system activity will be detected.

731 — Accuracy. The system must ensure that the correctness and consistency of
732 security-relevant information is maintained.

733 — Availability. System resources will be provided to users in a consistent and
734 reliable manner.

735 — Data Exchange. Data transmitted between system users and/or elements
736 will be protected from unauthorized interference or viewing. Originators
737 and recipients of data will be authenticated and will be able to mutually
738 prove their respective participation in the transaction.

739 **Nontechnical Security Objectives**

740 — Assurance. The security of the system must be specified, designed, imple-
741 mented, tested, and maintained in such a way that confidence can be
742 placed in the correct and effective operation of the system. Also, procedures
743 must be specified to ensure continued confidence in the security of the sys-
744 tem in the event that the system is modified in some manner.

745 — Security Roles And Responsibilities. Security activities must be partitioned
746 and allocated to identifiable security administrators who will then be
747 responsible for ensuring that their allocated task is satisfactorily per-
748 formed.

749 — Secure Operating Procedures. Procedures must be written that will guide
750 system administrators and users as to the correct procedure to follow in the
751 event of some security-relevant occurrence.

752 **5.2.4.1 Application Programming Interface Services**

753 **POSIX Security Interfaces**

754 The P1003.6 scope is limited to security extensions for those interfaces defined
755 within the base POSIX interface specification (POSIX .1 {2}). Issues not addressed
756 within the P1003.6 scope include noninterface-specific architectural assurance
757 issues and communications security.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

POSIX Security Interfaces

The POSIX security interfaces will support Audit, Privilege, Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Information Labels (ILs). Implementation support for these POSIX security interfaces is optional.

The audit interfaces support the concept of accountability wherein all system users are made accountable for their actions through the recording of user identities and associated actions within an audit trail. The audit interfaces support both portable audit generating and processing applications.

The privilege interfaces support the enforcement of a least privilege security policy wherein system administration responsibilities and associated privileges are allocated to a number of discrete roles, in order to compartmentalize the security impact of a subverted security administrator or of unauthorized usage of a security administrator role.

The DAC interfaces support the imposition of a fine granularity of user specified access control to objects. The DAC interfaces supplement the user-group-other permission bits that currently exist within the UNIX system through the use of Access Control Lists (ACLs).

The MAC and IL interfaces support the imposition of system specified policies for labeling. A MAC label is associated with an object (e.g., a file) and is typically used for access control purposes. An information label is associated with the data contained within the actual object itself and may therefore be used as a more accurate label for the purposes of hard copy printing. Further, an IL may contain information that is not related to logical access control and that is therefore not suitable for inclusion within a MAC label; e.g., physical document handling restrictions.

5.2.4.2 External Environment Interface Services

FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.

5.2.4.3 Interapplication Software Entity Services

FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.

5.2.4.4 Component Management Services

FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

795 ### 5.2.5 Standards, Specifications, and Gaps

796 #### 5.2.5.1 Related Standards in the POSIX OSE

797 ISO 7498-2, *Information Processing Systems—Open Systems Interconnection Refer-*
798 *ence Model, Security Architecture.*

799 *Information Retrieval, Transfer And Management For OSI—Draft Access Control*
800 *Framework, ISO/IEC SC21/WG1.*

801 *ISO/IEC 8613, Information Technology—Text and Office Systems—Office Docu-*
802 *ment Architecture (ODA) And Interchange Format.*

803 Draft Addendum to ISO 8613 On Security

804 CCITT X.509, *Message Handling System, ISO/CCITT X.400 Directory Authentica-*
805 *tion Framework.*

806 ECMA CMA 138, *Security In Open Systems—Data Elements And Service*
807 *Definitions.*

808 *Card And Card Terminals, European Telecommunications Standards Institute,*
809 *Terminal Equipment TE9*

810 #### 5.2.5.2 Related Documents in the POSIX OSE

811 *The Information Technology Security Evaluation Criteria,* Version 1.2, 28 June
812 1991.

813 US DoD, DOD 5200.28-STD, *Trusted Computer System Evaluation Criteria.*

814 Trusted Network Interpretation

815 Trusted Database Interpretation

816 Computer Security Subsystem Interpretation

817 #### 5.2.5.3 Emerging Standards in the POSIX OSE

818 To be provided.

819 #### 5.2.5.4 Related Standards

820 To be provided.

821 #### 5.2.5.5 Gaps in Available Standards

822 To be provided.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

823 **5.2.6 OSE Cross-Category Services**

D

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.3 Information System Management

Responsibility: Don Folland, Neil Croft D

DEF : The following is outline material as place-holder for more substantive text.

5.3.1 Overview and Rationale

The following issues should be addressed in subclauses 5.3.1 and/or 5.3.2:

— should support a variety of system management support scenarios (central management, dispersed management, or hybrid)

— this section should address both distributed systems and standalone systems.

— could be applied to Application Software or software components of the application platform.

— support automated management and operation of the IT infrastructure

— should address a wide variety of licensing scenarios

5.3.2 Scope

This category includes services and policies that address the administration of the overall information system required by any organization, including:

— Information Management

— Processor Management (e.g., Add new user)

— Network Management

— Configuration Management

— Security Management (e.g., Authentication, Key Management)

— Accounting Management

— Performance Management

Administration services accessible from the API may have Programming Language or Language Binding service specifications associated with them.

These services are defined to provide system and network administrator portability.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.3.3 Reference Model

< Consistent with Draft 11 Section 3.0 >

5.3.4 Service Requirements

The following services are required:

5.3.4.1 Software Installation and Distribution D

The main types of software to be installed and distributed are application programs developed in-house, bought-in applications, and utility software and personal computer software packages. All software needs to be managed effectively from development or purchase through to the live environment. Unless the distribution and implementation process can be controlled automatically, or from the center using software tools, procedures must be in place to ensure that distributed software arrives when expected and is checked for authenticity in whatever way is practical, and that the software is brought into use when required. The main procedures involved in software distribution and installation are:

— Central Software Control and Distribution (SC&D) staff to inform remote staff when to expect distribution software to arrive.

— Recipients to report to central SC&D staff when the distributed software has arrived successfully.

— Central SC&D staff to check that all software is received as expected at locations.

— Central SC&D staff to issue clear instructions about when the software is to be implemented.

— Location staff to report to SC&D when the software has been implemented. The release record on the Configuration Management Database will state which installations are to receive the release. This database must be updated to reflect the receipt and implementation of the release at each site.

5.3.4.2 License Services D

The terms and conditions relating to the supply of software may place legal restrictions on the organization (e.g., no unauthorized copies to be made). It is particularly important therefore that the Configuration Management Database is updated with details of who holds copies of software items. This assists the organization in discharging its legal obligations and assists auditors in checking for the existence of unauthorized copies.

All authorized copies of licensed or purchased software that are made by SC&D staff must be allocated a unique copy number and recorded in the Configuration Management Database together with where they are located and who is responsible for them. Procedural restrictions should be introduced to prohibit the

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.