NIST Special Publication 500-232

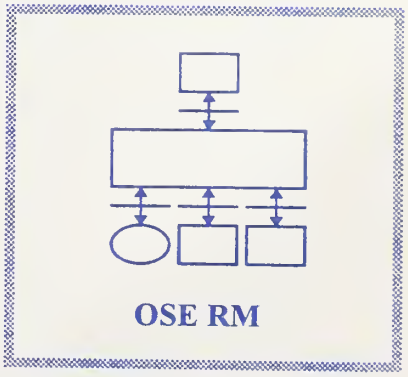
Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

Open System Environment (OSE): Architectural Framework for Information Infrastructure

Frederick (Fritz) Schulz



The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Office of the Director
- Advanced Technology Program
- Quality Programs
- International and Academic Affairs

Technology Services
- Manufacturing Extension Partnership
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Kinetics and Thermodynamics
- Analytical Chemical Research
- Process Measurements[2]
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Intelligent Systems
- Manufacturing Systems Integration
- Fabrication Technology

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Safety
- Fire Science

Computer Systems Laboratory
- Office of Enterprise Integration
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 500–232

Open System Environment (OSE): Architectural Framework for Information Infrastructure

Frederick (Fritz) Schulz

Systems and Software Technology Division
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-232
Natl. Inst. Stand. Technol. Spec. Publ. 500-232, 47 pages (Dec. 1995)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1995

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Foreword and Acknowledgments

This document represents a collaboration among the sponsor agencies for the National Institute of Standards and Technology (NIST) Distributed Systems Engineering Program. The following agencies and individuals contributed their time, experience and documents to the development of this document:

- Department of Defense	
Assistant Secretary of Defense for C3I - DASD(IM)	Mr. Terry Hagle
DISA Center for Architecture	Mr. John Mitchell
- Federal Aviation Administration	
Office of the Chief Information Officer	Mr. Roger Cooley
- Internal Revenue Service	
Office of Systems Engineering	Mr. John Tucker
- National Aeronautics and Space Administration	
Johnson Space Center	Mr. David Pruett
Goddard Spaceflight Center	Ms. Martha Szczur
- National Institute of Standards and Technology (NIST)	
Mgr., Distributed Systems Engineering Group	Mr. Fritz Schulz

This document draws from the agency experience and planning documents related to the establishment of large scale distributed systems which support their agency mission. The information infrastructure is viewed as an integral element of each of these agencies information technology programs.

In addition to the contributions of those above, special thanks to Jim Turnage (DoD DISA Center for Architecture) and David Farley (IRS) who made contributions to the development of this document. The following NIST personnel contributed or identified source material in the following areas: Barbara Cuthill (Software Development), Joe Hungate (Distributed Systems Management), Will Frazier (Security) and Brenda Gray for her editorial skills, as well as for their review of the overall document. This document also benefited from substantial review and comment from David Jefferson, Bruce Rosen, and Sheila Frankel of NIST.

Contributions are also drawn from across the OSE community, including business, government, and the consensus process organizations. The OSE concept has evolved and grown over the past seven years as a collaboration among many organizations and forums. In addition to the agencies above, special thanks should go to the information technology user and provider organizations which participated in the IEEE Posix 1003.0 working group (known as "dot zero"), ISO/IEC SC 22 Working Group 15 (the international forum for Posix), ISO/IEC JTC1 Special Group on Functional Standards (responsible for JTC1 profiles). The regional workshops, including the European Workshop for Open Systems (EWOS), the OSE Implementors Workshop (OIW) for North America, and the Asiatic/Oceana Workshop (AOW), provided input, feedback, and a crucial connection to those deploying information technology. Finally, thoughtful review and comment were received from the two organizations active in defining the U.S. approach to information infrastructure. The U.S. Government's Information Infrastructure Task Force (IITF) refined and focused the relationship between a relatively small system serving a single organization, and the larger infrastructure. The industry-led Information Infrastructure Standards Panel (IISP) sponsored a very useful review and "field trial" of the six interfaces defined in the August 1994 version of this paper.

With such a large and diverse community of discourse, a full list of contributors would be almost impossible to create. Any oversight is regretted.

PREFACE

This architectural framework document is one of a series of reports which together will provide a comprehensive overview of the National Information Infrastructure (NII) issues from the three different perspectives identified by the Information Infrastructure Task Force (IITF). The May, 1994, IITF report "Putting the Information Infrastructure to Work" provides a "top-down" (or applications) perspective. A "bottom up" (or bitways) view is presented in a July, 1994, Draft of "Framework for National Information Infrastructure Services." This report is presented from the third perspective, a services/interfaces centered view of the NII. Each of these reports, by itself, provides a critical view of the NII services and architectural framework, but it is only when viewed from all three perspectives that the true complexity and scale of the NII challenge emerges.

Significant Changes Since Version 1, August 5, 1994

- New versions of the reference documents resulted in updated terminology, especially in section 6, addressing the profiling process.
- Discussion and changes proposed by Information Infrastructure Task Force and the Information Infrastructure Standards Panel are reflected here, in the treatment of the Network-to-Network Interface (NNI).
- "National class" has been changed to "large scale."
- "NII" has been changed to "information infrastructure."
- Sections 5.4 "Software Development Capabilities," and 5.3 "Distributed System Management Capabilities" were substantially updated.
- Section 6 "The Profiling Process: Standards and Specification Selection" was rewritten with additional text describing the types of documents available.
- New text was inserted into section 7 "Summary and Conclusions."

Table of Contents Page

Table of Figures Page

1. Introduction

1.1 Scope

This document identifies a set of interfaces, services, and formats which are to be provided to users of an information infrastructure, and the methods for accessing these services. These interfaces, services, and formats describe an Open System Environment (OSE), enabling the existing and emerging information infrastructure for the communications, computing, and entertainment arenas to seamlessly interoperate.

One purpose of this formulation of the services is to provide a foundation for the selection of the information technology standards necessary to satisfy information infrastructure related objectives. Only the minimum set of services which are required to meet information infrastructure objectives (listed in section 2) is identified within this document. Concepts which must be agreed upon among all system constituencies are identified, and any concept or issue which can be left to a more localized authority is explicitly out of scope for this document.

This document provides a context and guidance for standards selection, but does not identify standards for use within an information infrastructure. The document may, however, refer to standards in order to illustrate aspects of the services which are important in making selections among the candidate specifications.

This discussion will provide a basic set of terminology and concepts to support discussion and resolution of policy issues.

Finally, technical guidance is provided to agencies which intend to use information infrastructure for exchange of government information and services within government, and to deliver government information and services to citizens and organizations outside of government.

1.2 Purpose and Audience

The purpose of this document is to identify a range of information infrastructure services and provide a context for standards selection. The issues involved in service and standards formation are closely related to policy issues such as intellectual property considerations and regulation. Information technology and technology policy evolve in parallel, and affect each other. This document provides a focal point for assessing the policy options as the technology and consumer expectations evolve.

The establishment of any distributed system which spans multiple organizations requires agreement among those organizations on a few key issues. These agreements are often codified as standards, but can take other forms, such as convention, registries, or regulation.

This document begins with an identification of the NII principles and objectives which will guide the evolution of the infrastructure, in section 2. This is followed by a set of capabilities that need to be established to satisfy the information infrastructure principles and objectives. Section 3 identifies a basic context and terminology that allows a clear statement and discussion of the issues. Types of services are identified, and the relationships among a few key concepts are outlined.

Sections 4 and 5 identify the information infrastructure services which must be addressed by the broadest community. Section 4 describes a general set of service requirements by identifying the services needed at several key interfaces. Section 5 addresses system level services; that is, those capabilities which cannot be isolated to a single interface.

Section 6 identifies a process and selection criteria which can be used to identify and select among candidate specifications which potentially satisfy the service requirements.

2. Architectural Framework Guidelines and Objectives

According to the Information Infrastructure Task Force report, "The National Information Infrastructure: Agenda for Action,"[1] the information infrastructure will include a wide variety of equipment with differing capabilities and services including "cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers, and much more." The services identified in this architectural framework will include services applicable to all identifiable service providers. The services will be those necessary for interoperability and portability between these diverse service providers and service users, with little distinction drawn between service providers and service users.

The architectural framework will ensure that organizations will be able to "integrate and interconnect these physical components in a technologically neutral manner so that no one industry will be favored over any other."[1] The services architecture will "assist service providers and users in the development of quality elements of information infrastructure including:

- The information itself, which may be in the form of video programming, scientific or business databases, images, sound recordings, library archives, and other media. Vast quantities of that information exist today in government agencies and even more valuable information is produced every day in our laboratories, studios, publishing houses, and elsewhere;

- Applications and software that allow users to access, manipulate, organize, and digest the proliferating mass of information that the NII's facilities will put at their fingertips;

- The network standards and transmission codes that facilitate interconnection and interoperation between networks, and ensure the privacy of persons and the security of the information carried, as well as the security and reliability of the networks;

- The people -- largely in the private sector -- who create the information, develop applications and services, construct the facilities, and train others to tap its potential. Many of these people will be vendors, operators, and service providers working for private industry."[1]

2.1 NII Principles and Objectives

The following NII principles and objectives from "The National Information Infrastructure: Agenda for Action,"[1] are relevant to the definition of services for large scale distributed systems:

1. Promote Private Sector Investment;
2. Extend the "universal service" concept to ensure that information resources are available to all at affordable prices;
3. Act as catalyst to promote technological innovation and new applications;
4. Promote seamless, interactive, user-driven operation of the NII:
5. Ensure information security and reliability;
6. Improve management of the radio frequency spectrum;
7. Protect intellectual property rights;
8. Coordinate with other levels of government and nations;
9. Provide access to government information and improve government procurement.

2.2 Technical Capabilities

In order to assure technical feasibility and credibility of this guidance, technical capabilities are identified as objectives. The architectural framework will describe capabilities and services which citizens and industry can use to access a wide variety of information from government agencies, as well as many other sources. The services will be as independent as possible of information content so as to provide general access capabilities. The following technical capabilities are taken from the IEEE/ISO "Guide to the POSIX Open Systems Environment."[2] This set of capabilities is in use in a variety of U.S. and International Open System Environment (OSE) related activities, and provides important support to the satisfaction of the objectives in section 2.1:

1. Application Portability at the Source Code Level;
2. Data Portability;
3. Application Software Interoperability and Application Platform Interoperability;
4. Common Methods for People to Interact with Technology;
5. Accommodation of Standards;
6. Accommodation of New Information System Technology;
7. Application Platform Scalability;
8. Distributed System Scalability;
9. Implementation Transparency;
10. Clear Statement of User Requirements.

2.3 Application Area Issues

The following application areas identified in "Putting the Information Infrastructure to Work,"[3] in "The Information Infrastructure: Reaching Society's Goals,"[4] and "R&D for the NII: Technical Challenges"[5] symposium proceedings, (see bibliography, Annex B) and will be used to validate that the services identified are broadly useful:

1. Health Care,
2. Education,
3. Manufacturing,
4. Electronic Commerce,
5. Environmental Monitoring and Information Dissemination,
6. Government Information and Services,
7. Libraries,
8. Electric Power Generation and Distribution,
9. Transportation,
10. Telecommuting,
11. Emergency Management,
12. Arts, Humanities, and Culture,
13. Law Enforcement and Criminal Justice.

While the selection of a small set of application areas is necessary to focus these service definition activities, it is recognized that there are many other important application areas. A collection of important issues common to these application areas could be a useful approximation of issues relevant to all application

areas. The application area issues identified in "Putting the Information Infrastructure to Work"[3] and "The Information Infrastructure: Reaching Society's Goals"[4] include:

- Equity of Access;
  Each persons ability to participate as a full citizen in our Republic should be enhanced, rather than lessened by technological change. Therefore, sensory and mobility impaired citizens must be included in our vision of the NII. Non-profit and private organizations must also be included in this vision of the NII, in addition to for-profit organizations.

- Demonstration and Pilot Projects;
  Demonstrations will reduce risk and verify cost/benefit projections, allowing better return on investment.

- Standards and the Standards Process;
  Clear goals and coordination will enable the voluntary standards system to work to maximum efficiency in identifying relevant existing standards, and developing any new standards required. New mechanisms, structures, and processes can improve standards development, resulting in more timely response to user needs.

- Privacy and Communications Security;
  Users must have some assurance of the identity of their communicating partner, and assurance that communication is available only to intended parties.

- Training and Support;
  Without adequate provision for ease of use and training for professionals and those they serve via the NII, the projected benefits of the infrastructure will not be achieved.

- Research and Development;
  Research should be funded and structured to support and sustain the current high rate of innovation and benefit from the NII.

- Performance Measurements;
  Measures of success should be defined to monitor the actual costs and benefits accrued from the NII, and to enable more intelligent investment changes along the way.

- Technologically Robust Architecture;
  A specialized infrastructure which accommodates a limited set of capabilities (e.g., more entertainment on television) would miss opportunities associated with trends toward decentralization, connectivity across heterogeneous networks, and radically different services.

- Diversity of Content;
  The infrastructure should allow for all types of cultural exchange, in addition to accommodating the dynamics of commercial exchange.

- Safety in our Homes and Protection of our Neighborhoods;
  The NII has the potential of improving coordination among community agencies in time of emergency, and increasing the exchange of information with citizens with concerns regarding the environment, transportation, and public safety.

- Citizen control over Private Information;
  Citizen control over the disclosure of private information held outside their direct control is essential to gaining their confidence, and realizing the benefits of the information infrastructure.

Figure 1 describes the relationship of technology infrastructure to application areas. The diagram makes the important point that it is not possible, nor desirable to establish a separate infrastructure for each application area. Many application areas will share a common infrastructure, represented by the "Services" and "Bitways" elements in the diagram. The architectural framework described in this document identifies the infrastructure which is common to many application areas.

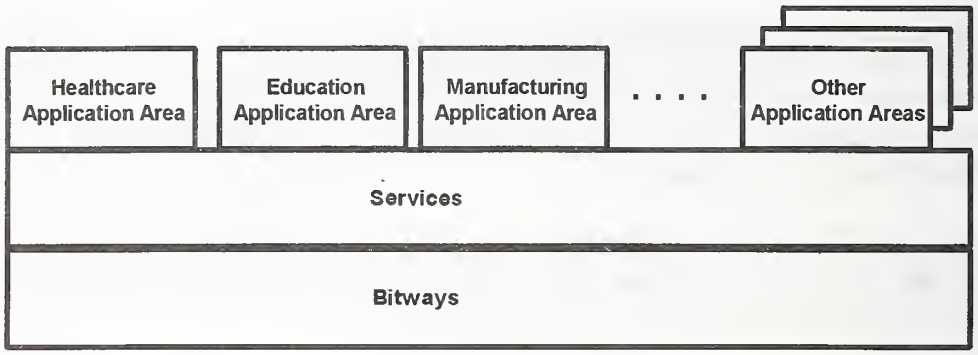


Figure 1: Relationship of Infrastructure to Application Domains.

3. OSE Architectural Framework

Today's large scale distributed systems, such as the Internet, are, and will continue to be composed of various smaller distributed systems bound together by very capable communications and support services. Each of these component distributed systems will be owned and operated by organizations (e.g., hospitals, schools, businesses, etc.). These systems will interact with each other in the transfer and sharing of data, but will not be obligated to respond to management directions from other organizations. The combined distributed system will not be provided, owned, or administered, by a single authority. It could continue to operate as a cooperative venture, with only a few carefully chosen unique authorities, such as domain registration authority.

The relationship of these systems may be described as *federated*. This federation is a voluntary, possibly transient, association between two or more complex systems. Each organization retains the responsibility for managing the system elements within the organization's scope, while allowing interaction with other systems in a carefully prescribed way. The process of establishing, operating, and evolving national class distributed systems is identified as Distributed System Engineering.

Current interactions are primarily confined to exchange of electronic mail messages, and in some cases remote session support. The variety of interactions available is rapidly expanding to include increasingly complex interaction between application programs on different platforms, often without the direct involvement of people. It is worth noting that even the NII itself is a component of a federated system due to its participation in a broader, global level distributed system.

3.1 Approach

The process of establishing large distributed systems which span multiple organizations requires a distinction to be made between an "architectural framework" and an "architecture." An *architectural framework* identifies key interfaces, entities and services, and provides a context for identifying and resolving policy, management, and strategic technical issues. The entities and interfaces provide a *reference model* that identifies the technology and provides a clear scope for specification. The framework constrains implementation by focusing on interfaces, but does not dictate design or specific technical solutions. An engineering organization then selects technology which implements the architectural framework, resulting in a specific design which is documented as an *architecture*.

This document describes an architectural framework for large scale information infrastructures. An overall architecture is not specified, since the variety of technology incorporated within the information infrastructure will vary considerably.

The framework may be tailored to address the needs of an organization which intends to depend on an external information infrastructure as a key component of the organization's own internal information infrastructure. This "project" perspective will help assure that pragmatic guidance is available to organizations with development projects and procurements always in progress. To this end, a simple set of terms will be developed to support the remainder of the document.

An important feature of this approach is that a method for capturing and tracking user requirements is integral to the process. This will help assure that technology and standards track user needs.

3.2 Technology Context - Open System Environment Reference Model

A distributed system is made up of elements of information technology which interact at specific locations. The following terminology and Open System Environment Reference Model (OSE RM) identifies the aspects of a distributed system which are relevant to technical policy discussions. These concepts and terminology are then used to identify the key interfaces where information infrastructure standards are needed.

Many of the initial concepts for the following were taken from the IEEE/ISO "Guide to the POSIX Open Systems Environment (OSE),"[2] developed during the period 1988 to 1995. NASA and the Department of Defense contributed the basic approach from infrastructure projects active during the period 1987 through 1989. Their partnership with the POSIX OSE project (P1003.0), helped to validate the concepts, to provide valuable feedback to their programs, and broaden the concepts so that they could make more extensive use of commercial technology. Another ISO/IEC project which provided important feedback was ISO/IEC JTC1 Technical Study Group 1 (TSG-1). This group, and their final report[6], established OSE (and profiling) as a major methodology within JTC1 for handling complex problems such as application portability.

3.2.1 OSE Reference Model - Canonical Form

A discrete, identifiable element of technology is identified as an *entity*. An entity may be made up of subsidiary entities, and may also be part of a larger entity. This document makes no naming distinction among entities with respect to where they fit in a hierarchy of such relationships since it is not necessary to support the policy discussion. As an element of technology, an entity is a "thing" and can be characterized in part by the technology used to implement it. For example, a candle and a light bulb are both implementations of a "light source" entity.

A boundary between two or more entities is an *interface*, with a location as an attribute. One method of characterizing a type of interface is to identify the entities which share the boundary. The distinction between entities and interfaces is an important one, since technical policy issues associated with interfaces and those associated with entities are quite different.

A *service* is a capability which a service provider entity makes available to a service user entity at the interface between those entities. Figure 2 illustrates how these three basic elements are graphically represented, and the relationships among them. This representation is the canonical form of the OSE reference model.

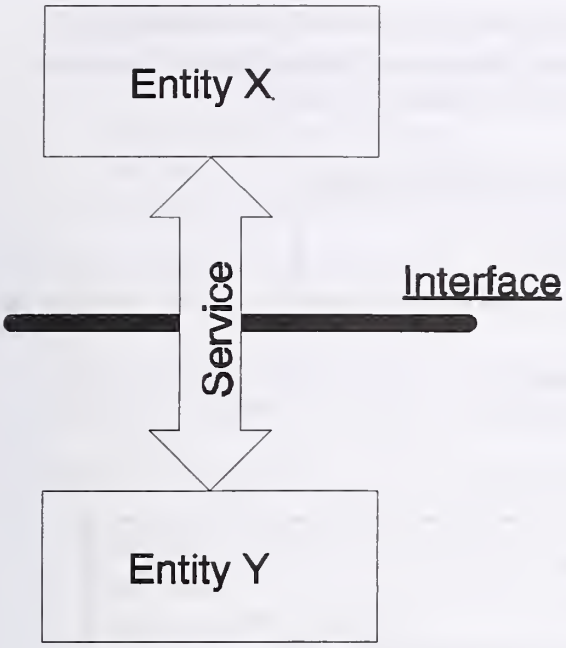


Figure 2: OSE Reference Model - Canonical Form.

A *service requirement* is a statement of need for a particular service at a specific interface. An *interface specification* is a document which specifies how a particular service is invoked or provided at a specific interface. Specifications are selected in response to a set of service requirements.

When a service requirement is identified for which no specifications are available, a *gap* in available standards is said to exist. Identification of gaps and filling gaps is a major challenge to organizations heavily dependent on distributed systems for their operation.

The reference model described can be used to identify the full range of information technology required to implement large scale distributed systems. However, it identifies only those features necessary to support policy discussions and formulation, or where consensus across all constituencies and participants is required. This minimal approach focuses on interface specification, and avoids mandating implementation to assure that the information infrastructure formulation accommodates the needs of the broadest range of application domains and technology solutions.

Note that the implementation of any systems participating in the information infrastructure may differ from the reference model presented. The objective is to define a conceptual reference model which allows widespread design, implementation, and integration communities to establish the necessary conventions and assumptions needed to fulfill their responsibilities. Partitioning of function for discussion or specification does not imply any requirement for similar partitioning in a specific design or implementation.

3.2.2 OSE Reference Model - Specific Interfaces and Entities

Using the concepts and terminology above, we now identify the specific interfaces involved in satisfying the objectives identified in section 2. The interfaces and entities identified are based on related projects and programs from industry, government, and the standards community. The model begins with a broad formulation (based on the "Guide to the POSIX Open System Environment"), and then adds further features from other contributions which address additional areas of interest. The discussion below is a distillation of the relevant parts of the referenced documents, and is intended to be a management summary. For a more detailed discussion, the reader is encourage to review the references listed in the bibliography (Annex B). A table in Annex A provides an initial identification of the interfaces included in a variety of reference models. Similarities among the interfaces identified in these documents suggest that a convergence on the definition and role of these interfaces is occurring.

Figure 3 depicts the specific Open System Environment (OSE) reference model. The model identifies five basic entities (blocks) and four types of interfaces (thick lines). Services are depicted as arrows crossing each interface. It is the characterization of these services that is the subject of section 4.

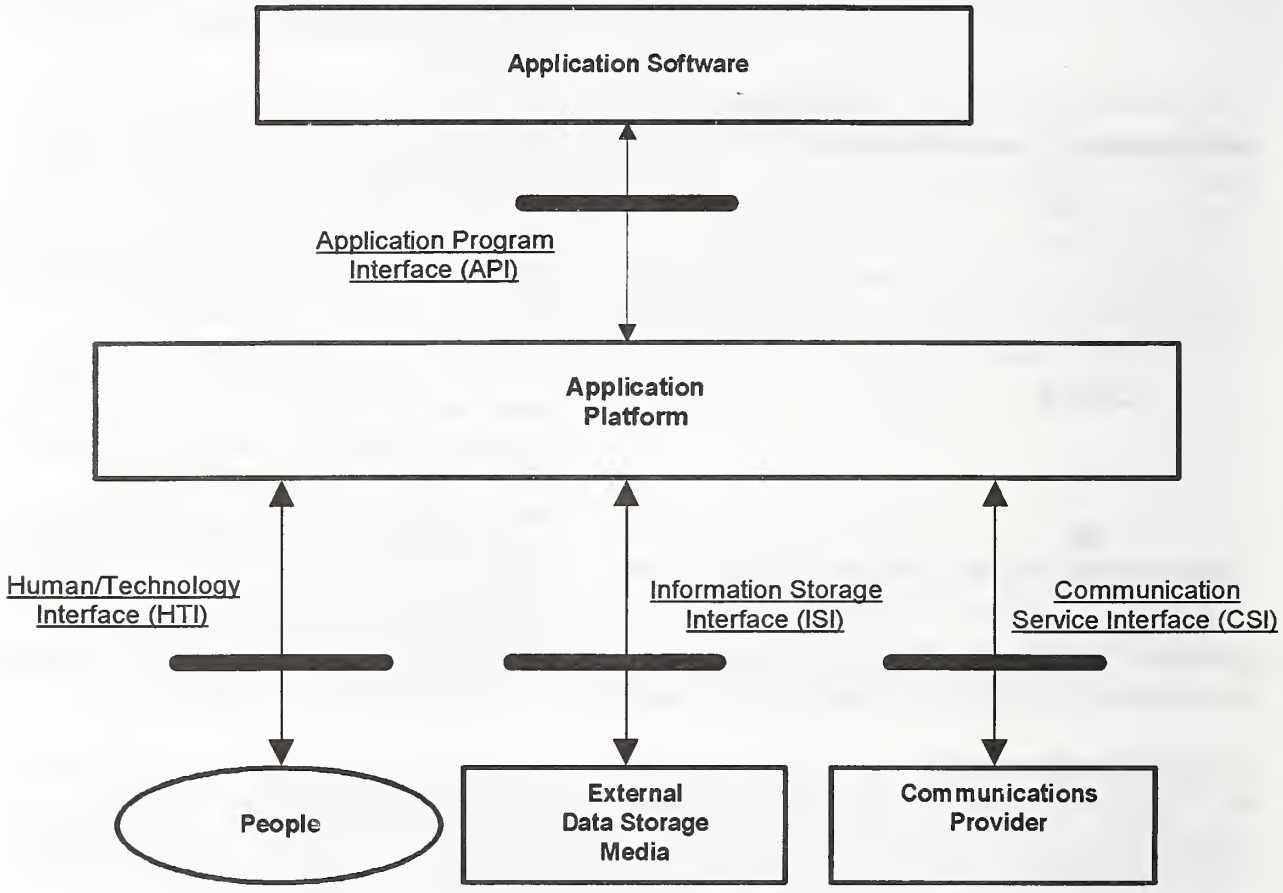


Figure 3: OSE Entities and Interfaces.

The interfaces will be described, with discussion of the entities included as needed.

An Application Program Interface (API) is the interface between an application software entity and an application platform, which is the immediate provider of all services necessary for execution of the application software entity.

Several types of specification are required and available at this interface. In general, any specification used by a programmer to generate application source code is an API specification. More recently, non-source code specifications such as language independent API specifications, and binary distribution formats have become available, to address the need for a non-development portability capability.

Justification for Inclusion: Specification at the API enables:

- application portability, supporting the user's need to manage investment in source code;
- vendor independent platform procurement, supporting equitable access to market for all suppliers;
- separate procurement of application platform and application software addressing legal, technical, economic, and regulatory issues;
- statement of API related intellectual property rights policy;
- application interoperability, which requires consensus on communications API specifications.

A Human/Technology Interface (HTI) is the interface across which people interact with information technology. The service provided is access to the information infrastructure, and to other people.

The types of specifications at this interface include human factors based descriptions of the events and capabilities available to a person interacting with information technology.

Justification for Inclusion: Specification at the HTI enables:

- reduced training cost, where common methods for invocation of identical or similar functions can be established;
- equal access for all citizens;
- users to choose among (or change) service providers, but still allows providers to differentiate their services and products;
- competitiveness, since ownership of fundamental HTI methods can provide advantage to one competitor.

An Information Storage Interface (ISI) is the interface across which information technology interacts with external storage media. The service provided is persistent storage of data, where the physical storage media is often removable.

The types of specifications at this interface include physical media and media independent data format specifications. The major policy issue is with media independent formats, but media is an important issue for government IT procurement and delivery of service to the citizen.

Justification for Inclusion: Specification at the ISI enables:

- migration from old technology media to new media, which is a steady state condition;
- available and affordable government information, which may require media distribution;
- the delivery and exchange of information, whether by network or by delivery of media, through consistent data format specifications;
- competitiveness, since ownership of basic storage methods can provide advantage to one competitor.

A Communications Service Interface (CSI) is the interface where an application platform accesses external entities which provide data transport services. The service provided is data transport among application platforms.

The types of specifications at this interface include those where protocol states, state transitions, data syntax, and data format are specified for interoperability among application platforms.

Justification for Inclusion: Specification at the CSI enables:

- regulation necessary to provide assurance of service;

- a necessary and fundamental consensus across a very large and diverse population of platform and communications service providers;
- competitiveness, since ownership of basic communications methods can provide advantage to one competitor.

The **Application Software** entity is software that is specific to an application, and is commonly referred to as an application program. For an organization developing application software, it may be represented by a human readable source code listing. For an organization buying application software, an application software entity may be represented by an executable file. Many organizations both develop and purchase application software. In either case, there may be data associated with the application program. If so, the data is considered part of the application software entity. An application software entity is the basic unit of procurement, development, and operation for an organization which uses software. A particular application may be characterized by the set of services it requires from the technology in order to execute, i.e., to perform its intended function.

The **Application Platform** entity is a set of resources, including hardware and software, that implement the services provided at the platform's interfaces. In particular, it directly provides all of the services to application software executing on that platform.

Application Software and Application Platform are often combined into one entity, referred to as an **Information Appliance (IA)**. This term is used where the presence of configurable and/or separately procurable software is not visible to the user of a particular component information technology. Examples of information technology which are currently considered IAs include telephones, set-top cable TV boxes, Video Cassette Recorders, television sets, fax machines, AM/FM radios, scanners, keyboards, computers of all kinds, computer monitors, printers, communications switches, routers, gateways, and cameras (film and video tape). Application platforms may be considered generalized information appliances. The relationship between Application Platform and Information Appliance entities is shown in Figure 4.

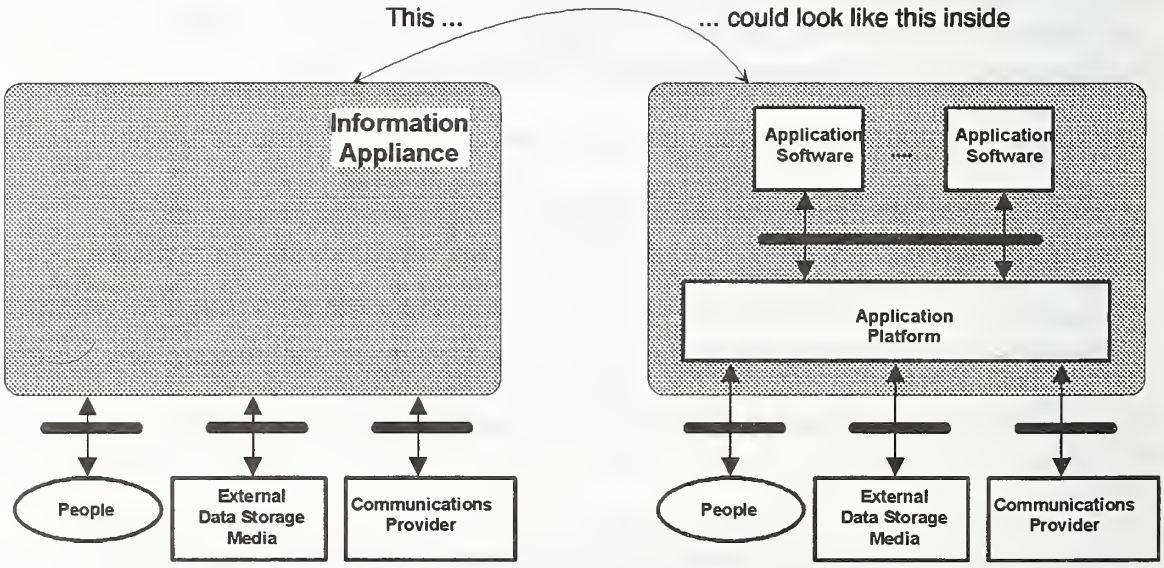


Figure 4: Application Platform and Information Appliance Entity Relationship.

The **External Data Storage Media** entity is a physical object which can be used to store and play back data from an application platform or information appliance. Examples of external storage media include floppy disks, audio and video cassette tape, and CD-ROMs.

People are, of course, one of the most important elements of any distributed system, as they usually represent the beneficiary of services offered by the system. People are represented as entities to assure that HTI methods and services are robust enough to support users needs. In some cases, people may also provide services directly via the NII in a manner similar to the way directory services operators provide services over the phone system.

The **Communications Infrastructure** entity is defined from the users perspective, where universal connectivity is provided to the full set of information appliances and people, nationally (and internationally). In reality the "Communications Infrastructure" is composed of a diverse set of alternative **Communication Networks** (CNs) , each associated with a single provider organization. Today, each of those CNs provide a variety of communication services to a specific (less than universal) group of users, using a variety of technologies. Examples of CNs include the long distance, regional, wireless, and local telephone switching systems, satellite systems, cable and radio frequency TV broadcast systems, and LAN/WAN service providers. The communications media used could be cable, optical fiber, microwave (or any part of the spectrum).

Each of the technologies has a different set of advantages and disadvantages, leading to their use in different situations. We should expect the diversity in Communications Infrastructure technologies, markets, and organizations to continue, but the policy objective of "universal connectivity" for some set of services leads to the need for interchange among Communication Network providers for that set of services.

A Network-to-Network Interface (NNI) is a type of interface where two or more (possibly dissimilar) communication networks exchange connectivity services, as shown in Figure 5. The service provided is communication connectivity to and from the population of information appliances and people directly accessible by other communication networks and their providers. The direct access population for a communication network and the associated provider is that set of appliances and people who can communicate among themselves without using any other service network provider. Both the Computer Systems Policy Project (CSPP) "Perspectives on the National Information Infrastructure: Ensuring Interoperability"[7] and the Cross Industry Working Group (XIWT), "An Architectural Framework for the National Information Infrastructure"[8] provide industry perspectives of this key interface.

The types of specifications at this interface include those where protocol states, state transitions, data syntax, and data format are specified for interoperability among providers of basic data transport services.

Justification for Inclusion: Specification at the NNI enables:

- universal access to all application services for the user, ensuring competition;
- universal access to the market for the application service provider, ensuring equity;
- competitiveness in the communications services market, allows user to choose among competing communications service providers.

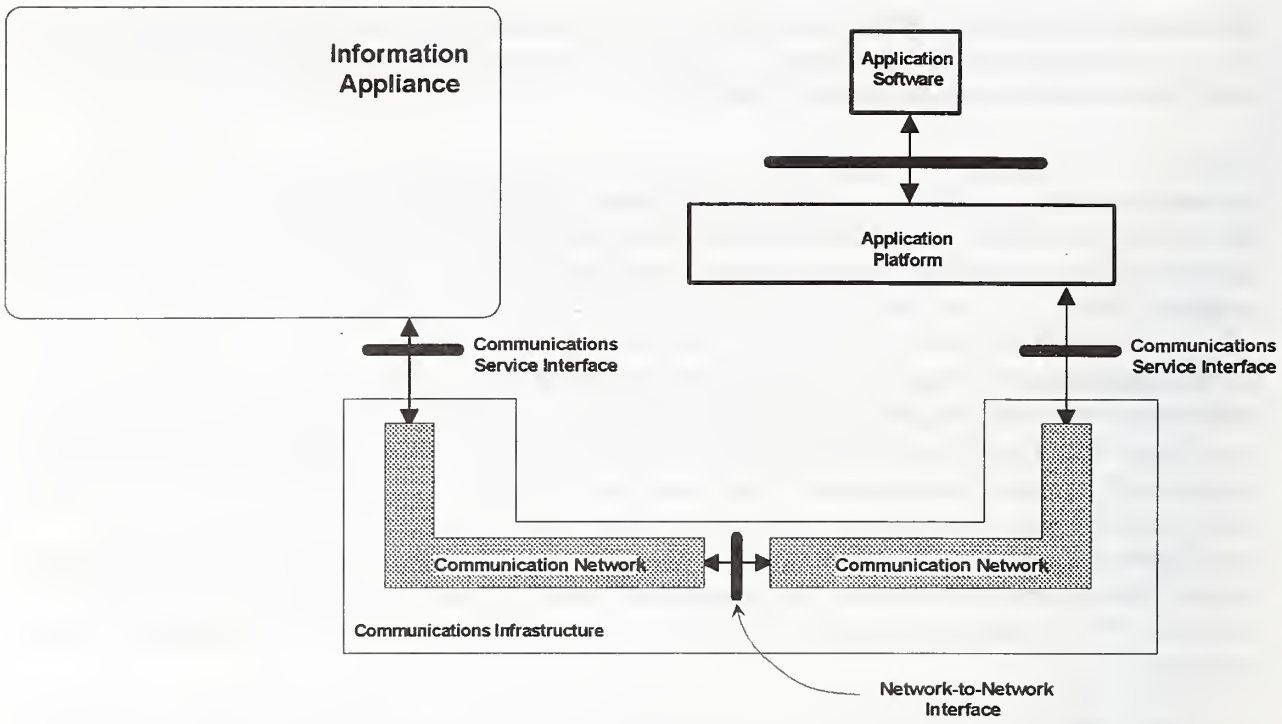


Figure 5: Network-to-Network Interface (NNI).

An Application-to-Application Interface (AAI) is a type of interface where an application software entity accesses services provided by other application entities. The service provided varies with the application accessed.

The types of specifications at this interface include specification of a basic data transport paradigm, a set of messages including syntax and semantics, specifications of allowed message sequence, and conventions for handling a variety of situations which may arise.

Justification for Inclusion: Specification at the AAI enables:

- competitiveness, since ownership of basic AAI methods can provide advantage to one competitor;
- universal access to the market for the application service providers, ensuring equity;
- universal access to all application services for the user, ensuring competition among service providers;
- Since many of the services being considered for "universal availability" are provided by application software entities, standards are required to support service access.

3.2.3 OSE Reference Model - Distributed System

The full OSE reference model, shown in Figure 6, identifies all of the interfaces and entities described above, and illustrates the relationships among them. In this abstraction of the full distributed system environment, multiple application platforms, each serving one or more applications, interact among themselves and with information appliances by way of common communications mechanisms. This collection of generic interfaces and entities can be used to represent key aspects of large distributed systems such as the internet.

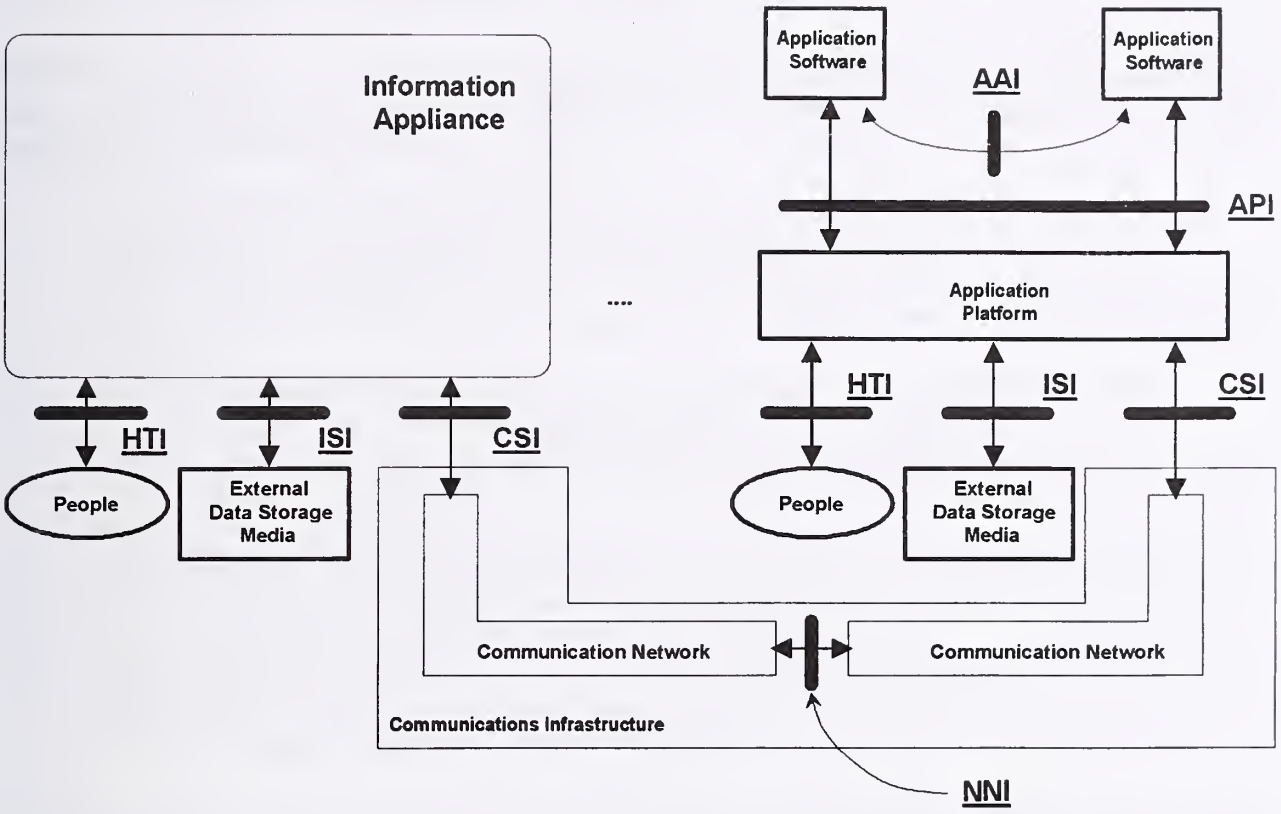


Figure 6: OSE Reference Model - Full Distributed System.

4. Service Definitions

This section defines the set of services needed at each of the interfaces defined above, in order to satisfy the guidelines and objectives identified in section 2. The services specified will be used to drive the selection of standards and other specifications. Services will be defined at a high level only to establish the scope of services for which standards are needed; this is not intended to be a complete set in the broadest sense.

4.1 Services at the Human/Technology Interface

Human/Technology Interface (HTI) services allow users to interact with information technology, and to tailor the HTI to their needs. Depending on the capabilities required by users and applications, services provided at this interface may include:

- Graphical Client-Server Services: allow a user to control the relationships between graphical user interface display client and server processes operating within a network;
- Display Objects Services: allow a user to control the characteristics of display elements such as color, shape, size, movement, graphics, context; user preferences; and interactions among display elements;
- Window Management Services: allow a user to control window creation, movement, storage, retrieval, and removal, and allow relationships among windows to be specified;
- Audio Services: allow a user to input, manipulate, and output sound, music, and other forms of audio. The services also allow the user to control aspects of the service such as volume, bandwidth, filtering, and storage allocation;
- Video Services: allow a user to input, manipulate, and output video. The services also allow the user to control aspects of the service such as resolution, bandwidth, filtering, and storage allocation. Synchronization of video and audio services may be required; and
- Dialogue Support Services: allow a user to control the definition of the relationships between what is displayed on the screen (e.g., cursor movements, keyboard data entry, external data entry devices) and how the display changes depending on the data entered.

User interfaces are a very complex part of system development and maintenance. Within the past few years, significant advances have been made in user interfaces, both in ease of use and in reducing the development effort required. Although other technologies can be used, most users think of a user interface in terms of a Graphical User Interface (GUI). A GUI allows a user to specify actions by dragging and dropping or pointing and clicking on an icon that is a pictorial metaphor of the object being acted upon. A GUI may also support several simultaneous threads of interaction by presenting multiple windows.

The principal components of a window system are a video display interface that contains one or more windows or panels; a pointing device, such as a mouse or touch-screen; and a set of visual objects on the screen that can be directly manipulated by the user through a pointing device or keyboard.

Internationalization services available at the Human/Technology Interface may include providing the user with the:

- Ability to select among character sets;
- Character set identifiers and formats;
- Character data presentation;

- Specialized character data input services;
- Ability to select among cultural conventions;
- Ability to select the primary language displayed;
- Ability to simultaneously support multiple language on the same display;
- Support of culture specific keyboards; and
- Support of culture and language specific messages, i.e., wording or icons that are appropriate to the users cultural conventions and mores. Applications should be independent of any particular natural language, presenting messages appropriate for the internationalized user environment selected by the user.

Special formulations of these services may be available for individuals with physical or sensory impairments.

Service availability may be restricted by configurable security or resource allocation constraints. Authentication services may be invoked one or more times during a usage session in order to limit access to system resources to authorized individuals, and to promote privacy on shared systems.

4.2 Services at the Information Storage Interface

The basic services offered at this interface are persistent storage of data, and data format specification for interchange. Two types of specifications required at this interface include physical media specifications and media independent data format specifications. Both are required to establish a capability for data portability and exchange of large volumes of data via media. Because the continued fast pace of improvement in storage technology shows no signs of slowing, it is important to consider methods for migration from legacy storage to new storage technology.

Physical media specifications identify the relevant physical characteristics of distribution media. These characteristics vary considerably with the media, including:

- Magnetic tape and disk;
- CD ROM; and
- Smart card and encryption support devices.

Media independent data format specifications identify all information required to read and interpret stored data. This begins with bit and byte order conventions, and extends to complex data types such as:

- Byte, integer, floating point, string, etc.;
- Compound types, i.e., records, tables;
- Graphics, animation, image, audio, video, with linkage and synchronization points among the various media identified; and
- Files, documents, etc.

Internationalization data formats defined at the Information Storage Interface include:

- Formats for defining character sets and character set identifiers;
- Collation sequences and character equivalency sets;
- Formats for defining cultural conventions; and
- Natural language message system formats.

Service availability may be restricted by configurable security or resource allocation constraints. Information stored on media may be encrypted to promote privacy on shared storage media. Ownership and authorization information may be required to support these security capabilities.

4.3 Services at the Communications Services Interface

The services at the application platform to communications infrastructure interface may include one or more of the following:

- packet and/or asynchronous bi-directional data transport with application platform or information appliance interface addressing;
- One, or more inbound audio data streams;
- One, or more outbound audio data streams;
- One, or more inbound video data streams;
- One, or more outbound video data streams;
- One, or more inbound synchronized audio/video streams; and
- One, or more outbound synchronized audio/video streams.

Individual stream bandwidth and aggregate bandwidth may vary, with automatic network accommodation up to a negotiable maximum.

The National Research Council report, "Realizing the Information Future"[9] points out that where bandwidth is not sufficient to satisfy all requests for services, communications service providers must select a strategy for allocating service. Generally, the provider must choose between imposing delays on users by adopting a best effort service strategy, or provide for negotiation of service where the traffic source declares its service requirements so that the network can either reserve and guarantee service or explicitly refuse the service request. Since this document is limited to definition of services, and will not address implementation, the above services are to be considered goals (see NRC, pg. 66, for a more detailed discussion).

Note that in implementing these services, voice and video may eventually be supported via the packet data service, but much of the current installed base of switched phone technology does not support this service.

The National Research Council report proposes the migration to a single unified service at this interface, where a specified range of qualities of service is supported. The Open Data Network "bearer service" is defined in an abstract way that decouples the service characteristics from any particular technology choice. The various qualities of service are differentiated by reliability, timeliness, correctness and bandwidth of delivery.

Service availability may be restricted by configurable security or resource allocation constraints. Authentication services may be invoked one or more times during a usage session in order to limit access to system resources to authorized individuals, and to promote privacy on shared systems. Encryption services may be requested during communications operations to promote data confidentiality as information may transit shared systems.

4.4 Services at the Application Program Interface

This section describes those services provided to an application program by the underlying application platform.

4.4.1 Human/Technology Interaction API Services

These services allow an application program to interact with people at the human/technology interface. The operations supported may include:

- Window manipulations, such as open, close, move, resize;
- Operation of standard controls such as menus, and dialog boxes;
- Invoke execution of command language script;
- Manipulation of audio, video and other multi-media operations at the human/technology interface;
- Reading input from, and controlling keyboards and pointer devices; and
- Querying HTI technology to determine (and set) configuration parameters such as resolution, and sampling rates.

Specialized Graphics operations and services to an application program include:

- Create, delete, and modify features on a display. Features include:
  - -- Lines and Polylines (i.e., multi-segment lines);
  - -- Markers;
  - -- Regions, or fill areas;
  - -- Display Text and Annotation text;
  - -- Mesh Surfaces, such as Cell, Triangle strips, and/or Quadrilateral mesh;
  - -- Surfaces;
  - -- Curves;
  - -- Conics, such as circles, ellipses, parabolas, and hyperbolas; and
  - -- Models of objects to be displayed.

- Image manipulation;
- Control and apply color to features;
- Apply lighting and shading algorithms to collections of graphical objects with multiple light types and sources;
- Specify and edit the features and attributes globally and individually;
- Transformation of (i.e., scale, translate, rotate, reflect, project, etc.) primitives for construction of more complex objects and for arrangement in the viewing space;
- Store and retrieve graphical objects from files; and
- Control the timing of the actual display of the display data.

All Graphics operations and services may be required to support both two and three dimensional systems.

Internationalization services available at the Human/Technology Interaction API include providing the application program with the ability to:

- Select among character sets;
- Control character data presentation;
- Provide specialized character data input services;

- Select among cultural conventions;
- Select the primary language displayed;
- Simultaneously support multiple language on the same display;
- Support of local keyboards; and
- Support of natural language message system, i.e., wording or icons that are appropriate to the user's cultural conventions and mores. Applications should be independent of any particular natural language, presenting messages appropriate for the internationalized user environment selected by the user.

Service availability may be restricted by configurable security or resource allocation constraints. Authentication services may be invoked one or more times during a usage session in order to limit access to system resources to authorized individuals, and to promote privacy on shared systems.

4.4.2 Information Storage API Services

These services allow an application program to control and manipulate files and information associated with persistent storage resources. The operations supported include:

- File system services such as open, read, write, close;
- Determine and/or set file attributes such as ownership, privileges, etc.;
- Hierarchical directory structure operations such as set default directory, list files, etc.; and
- Media control operations such as eject media, load, rotate platen, format, etc.

These services also allow an application program to control and manipulate databases and structured data associated with persistent storage resources. The operations supported include:

- Database services such as open, query, add data, update data, delete data, close;
- Determine and/or set database and data attributes such as ownership, privileges, etc.;
- Determine and/or set relationships between a database and file systems, etc.; and
- Structure data access services.

Service availability may be restricted by configurable security or resource allocation constraints. Encryption services may be requested during storage or retrieval operations to promote privacy on shared systems.

4.4.3 Communications API Services

These services allow an application program to communicate with other application programs executing on the same or a remote application platform. A variety of different paradigms are available, each of which is useful for specific situations. The paradigms and operations supported include:

- Datagram message service:
  -- send message, receive message.

- Connection Oriented Messaging Service:
  -- Request connection to remote application;
  -- Send message, receive message via connection; and

-- Terminate connection to remote application.

In addition to these basic messaging services, conventions and specifications can be used to further refine the services offered. Two of the more widely used techniques include Remote Procedure Call, and Transaction Processing. Remote Procedure Call establishes conventions and specifications for semi-automated generation of source code for simple "request-response" interaction between application programs.

Transaction processing establishes conventions and specifications for conducting complex transactions among two or more application programs, with a high assurance of data and system integrity. Transaction processing operations supported include:

- Begin transaction;
- Commit transaction;
- Rollback transaction; and
- Failure recovery operation.

Service availability may be restricted by configurable security or resource allocation constraints. Encryption services may be requested during communications operations to promote data confidentiality, since information may transit shared systems.

4.4.4 System API Services

These services allow an application program to access resources within the application platform. The operations supported include:

- Core System Services:
  -- Application execution and concurrence control (for example for processes and threads);
  -- Event, error and exception management;
  -- Memory management;
  -- Local processor time;
  -- Platform internal communications and event synchronization;
  -- Determine and/or set processor configuration and environment; and
  -- Access control;

- Programming Language Services:
  -- Execution sequence (e.g. branching);
  -- Data type definition and memory allocation; and
  -- Arithmetic operations.

Service availability may be restricted by configurable security or resource allocation constraints.

4.5 Services at the Network to Network Interface

A Network-to-Network Interface (NNI) is an interface where one or more communication networks exchange connectivity services. While these services are not directly accessed by the end users, they benefit directly from the connection to the full population of service providers and people.

The services supported at the NNI include:

- data exchange at sufficient rates and volumes to satisfy end to end data transport service requirements;
- management, including participation in network fault detection, identification, isolation and recovery operations; and
- exchange of data required to support resolution of charges for service.

4.6 Services at the Application-to-Application Interface

Many of the services provided on distributed systems will be used by application software acting on behalf of a person. Application software entities exchange services with other applications using an application-to-application communications paradigm. An Application-to-Application Interface (AAI) specification specifies how an application software entity gains access to the services provided by another application software entity. The AAI should contain all the information required by an application programmer to either replicate the service or access the service from another application software entity. The application software entity which provides the service may be called a "server", and that convention will be adopted here.

The services provided by the following specialized servers, and AAI specifications for accessing their services, are needed to implement NII services. Service availability may be restricted by configurable security or resource allocation constraints. Authentication services may be invoked one or more times during a usage session in order to limit system access to authorized individuals, and to promote privacy on shared systems. Encryption services may be requested during communications operations to promote data confidentiality as information may transit shared systems.

4.6.1 Directory Services

A **Directory Service** provides network addresses and related information to applications. An application establishes communication with a directory server and identifies the application with which it will interact. The server returns the network address and related information about the destination application. Addresses at different levels may be requested and reported, including addresses for the application platform interface, application platform, or application software entity. The directory service may actually involve a variety of servers, each with varying scope and information content. Interaction with, and among, directory servers is documented in a Directory Server AAI specification.

4.6.2 Electronic Mail Service

An **Electronic Mail Service** provides a capability for a person or application software entity to exchange messages with other people or application software entities. A person may use any of a variety of specialized applications to compose a message, which may contain any combination of data, text, audio, video, graphics, and/or images. An application submits a message for electronic delivery by interacting with a mail server. Mail is forwarded to successive servers until the mail reaches the destination, at which point it is held until requested by the addressee. Interaction with, and among, mail servers is documented in an Electronic Mail Server AAI specification.

4.6.3 Time Synchronization Service

A **Time Synchronization Service** provides a capability for different application platforms on a distributed system to be synchronized to an accuracy that lies within an arbitrary clock error. Interaction with, and among, time synchronization servers is documented in a Time Synchronization Server AAI specification.

4.6.4 Remote Graphic User Interface Service

A **Remote Graphic User Interface Service** provides a capability for a person to interact with one or more applications which are executing remotely across the network, using graphical user interface techniques. The Remote Graphic User Interface Service may actually involve a variety of servers, each with a different role and area of concern. Interaction with and among Remote Graphic User Interface servers is documented in a Remote Graphic User Interface Server AAI specification.

4.6.5 Remote Login

A **Remote Login Service** provides a generalized capability for a person to interact with one or more applications which are executing remotely across the network, using character-oriented command line interface techniques. The Remote Login Service may actually involve a variety of servers, each with a different role and area of concern. Interaction with, and among, Remote Login servers is documented in a Remote Login Server AAI specification.

4.6.6 Authorization Service

An **Authorization Service** provides a capability by which a person or application software entity is associated with a set of privileges and/or resource limitations. An application establishes communication with an authorization server and identifies the person or application software entity to be checked, and the privilege invoked or resource requested. The authorization server returns an indication that the authorization request is valid or invalid. Interaction with, and among, authorization servers is documented in an Authorization Server AAI specification.

4.6.7 Authentication Service

An **Authentication Service** provides a level of assurance that a person or application software entity is actually the authorized agent identified. An application establishes communication with an authentication server and identifies the person or application software entity to be authenticated, along with authentication information, such as a password or biometric information. The authentication server returns an indication that the authentication is valid or invalid. Interaction with, and among, a specified set of authentication servers is documented in an Authentication Server AAI specification.

4.6.8 Non-Repudiation Service

A **Non-Repudiation Service** provides a level of assurance that a transaction carried out by an authorized person or application software entity will not be repudiated by any interested party. This service is similar to that provided by a Notary Public. Applications operating on behalf of parties wishing to enter into an agreement establish communication with a notary server. Parties with fiduciary responsibility to enter into an agreement are authenticated, and binding commitment to the agreement is registered with the notary server. The server distributes a copy of the agreement to all parties, including proof of commitment. Interaction with, and among, notary servers is documented in a Non-Repudiation Server AAI specification.

4.6.9 Data Integrity Service

A **Data Integrity Service** provides a level of assurance that the content of a set of data remains unchanged over a period of time. An application operates on the content of a file or other data set according to an algorithm designed to generate a unique value. The algorithm is not reversible, thereby protecting the original information from discovery. An application then establishes communication with a data integrity server and reports the integrity value, along with any desired attributes of the data, such as the person or application software entity to be associated with the data, or timestamp. Variations allow for integrity validation and time-stamping without disclosure of content for applications where protection of intellectual property, and establishing origin is important. The server can then provide confirmation of the integrity of copies, or substantiate claims of origination as needed. Interaction with, and among, Data Integrity servers is documented in a Data Integrity Server AAI specification.

4.6.10 Remote File Access Service

A **Remote File Access Service** provides a generalized capability for an application to interact with (i.e. read from, modify, add to) one or more files or file systems which are located remotely across the network. The service may actually involve a variety of servers, each with a different role and area of concern. Interaction with, and among, Remote File Access servers is documented in a Remote File Access Server AAI specification.

4.6.11 File Transfer Service

A **File Transfer Service** provides a generalized capability for an application to transfer one or more files between application platforms connected by the network. The service may actually involve a variety of servers, each with a different role and area of concern. Interaction with, and among, file transfer servers is documented in a File Transfer Server AAI specification.

4.6.12 Remote Database Access Service

A **Remote Database Access Service** provides a generalized capability for a person or application to query or update one or more databases which are located remotely across the network. The service may actually involve a variety of servers, each with a different role and area of concern. For example, one or more of the

databases may consist of metadata describing the content of other databases. Interaction with, and among, Remote Database Access servers is documented in an Remote Database Access Server AAI specification.

4.6.13 Unstructured Data Discovery

An **Unstructured Data Discovery Service** provides a generalized capability for a person or application to browse and search through a variety of unstructured data which may be available locally or from other systems on the network. Minimum restrictions on the format, amount, or structure may be placed on the data accessed. Services should provide support for:

- Hypertext support that includes network-transparent links, multiple fonts, inline graphics, and hypergraphic links;
- Intra-document and infobase searching;
- Translation of flat data formats to hypertext formats;
- Security, including limiting access by site or user;
- Digital signing of documents; and
- Encryption of documents for transmission.

The service may actually involve a variety of servers, each with a different role and area of concern. Interaction with, and among, Unstructured Data Discovery servers is specified in an Unstructured Data Discovery Server AAI specification.

5. Multiple Interface Capabilities

Organizations have many requirements which do not fall neatly on a single interface, but require the coordinated specification and use of a variety of services at several interfaces. These requirements are for complex capabilities which are often difficult to define with precision, but are fundamental to successful application of information technology in the real world.

For example, an organization will need to establish a capability for protecting key systems from damage, whether accidentally or intentionally inflicted. Part of satisfying the need for this very complex capability involves providing specific security related services at specific interfaces. For each of the sub-sections described below, one or more combinations of services in section 4 may be required to provide the capability described.

5.1 Security/Privacy Capabilities

Security services/capabilities are necessary to protect sensitive information in the information system. The appropriate level of protection is determined based upon the value of the information to the mission area end users and the perception of threats to that information. Information system security services are depicted as cross-area services since the mechanisms implemented to provide them may be part of multiple platform service areas.

The following are security services that fall into this category:

- Authentication Service confirms the identities of requesters for use of information system resources. In addition, authentication can apply to providers of data. The authentication service may occur at the initiation of a session or during a session.

- Access Control Service prevents the unauthorized use of information system resources. This service also prevents the use of a resource in an unauthorized way. This service may be applied to various aspects of access to a resource (e.g., access to communication to the resource, the reading, writing, or deletion of an information or data resource, the execution of a processing resource) or to all accesses to a resource.

- Data Integrity Service ensures that data is not altered or destroyed in an unauthorized manner. This applies to data in permanent data stores and to data in communications messages.

- Data Confidentiality Service ensures that data is not made available or disclosed to unauthorized individuals or computer processes. This service will be applied to devices that permit human interaction with the information system. In addition, this service will ensure that observation of usage patterns of communications resources will not be possible.

- Non-Repudiation Service ensures that entities engaging in an information exchange cannot deny being involved in the exchange. This service may take one or both of two forms. First, the recipient of data is provided with proof of origin of the data. This protects against any attempt by the sender to falsely deny sending the data or its contents. Second, the sender of data is provided with proof of

delivery of data. This protects against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

- Availability Service ensures that timely and regular communications services are available. These services are intended to minimize delay, or non-delivery of data passed on communications networks. These services include protecting communications networks from accidental or intentional damage, and ensuring graceful degradation in communication service.

5.2 Internationalization Capabilities

An information infrastructure should provide services that are necessary to support users, irrespective of their particular natural language or cultural conventions. This supports both the need to accommodate cultural diversity, and the reality of using the information infrastructure as a vehicle for doing business in the global marketplace. While it is not expected that every application platform would provide support for all possible natural languages and cultural conventions, the specification of the information infrastructure services and the interfaces should not preclude such support.

Users may require the simultaneous support of multiple natural languages and cultural convention sets. Therefore, the basic information infrastructure internationalization requirement is to provide a set of services and interfaces that allow the user to define, select, and change between different culturally related application operating environments supported by the particular implementation. Specifically, a user should have the capability to:

- Adjust the output messages of specific functions and utilities to support different natural languages, cultural conventions and character sets;

- Select an internationalized user environment that specifies a particular set of data presentation characteristics, including cultural conventions, character sets and native language;

- Concurrently support different applications functioning in different internationalized user environments, supplying different sets of natural languages, cultural conventions and character sets for different users; and

- Support different internationalized user environments, and the associated natural languages, cultural conventions and character sets, without requiring changes to the logic of existing application programs.

The effect of the user selecting a new internationalized user environment, and its associated natural language, cultural conventions and character set, should be transparent to application programs.

Internationalization services are provided at the Human/Technology Interface, and the Application Program Interface. Internationalization data formats including character sets, cultural conventions, and natural language support messages are identified at the ISI.

5.3 Distributed System Management Capabilities

Management services are integral to the day-to-day operation of large scale distributed systems. They provide the mechanisms to monitor and control the operation of individual applications, file systems, databases, platforms, networks, and user interaction elements of distributed systems.

Activities required for the operations and administration of distributed systems can take on a very broad scope. This scope can be as simple as a single open system taking management responsibility for one or more dependent systems, or as complex as those in which there is a transient negotiated division of management activities. The prescribed manner in which these activities occur between systems determine important aspects of their relationship.

Services required for management of distributed systems are not fully defined. Open System Interconnection (OSI) Network Management and POSIX system administration functions (e.g., user accounts, resource administration, etc.) need to be integrated to provide a comprehensive set of management and administration services. Data and database administration, and other capabilities need to be integrated as well. The required services, based on those identified by the OSE Implementors Workshop[10], include the following:

- Application Software Management Services, including:
  - -- State Management (e.g., Startup and Shutdown);
  - -- User and Group Identification;
  - -- Configuration Control;
  - -- Service Access Control;
  - -- Usage Management and Cost Allocation (Accounting);
  - -- Performance Management;
  - -- Fault Management;
  - -- Security Management;
  - -- License Management; and
  - -- Software Installation and Distribution.

- Application Platform Management Services, including:
  - -- State Management (e.g., Startup and Shutdown);
  - -- User and Group Identification;
  - -- Configuration Control;
  - -- Service Access Control;
  - -- Usage Management and Cost Allocation (Accounting);
  - -- Performance Management;
  - -- Fault Management;
  - -- Security Management; and
  - -- Print Management.

- Human/Technology Interface (HTI) Management Services, including:
  - -- State Management (e.g., Startup and Shutdown);
  - -- User and Group Identification;
  - -- Configuration Control;
  - -- Service Access Control;
  - -- Usage Management and Cost Allocation (Accounting);
  - -- Performance Management;

-- Fault Management; and
-- Security Management.

- Information Management Services[11], including:
  -- Database Management (including Data Administration);
  -- State Management (e.g., Startup and Shutdown);
  -- User and Group Identification;
  -- Configuration Control;
  -- Service Access Control;
  -- Usage Management and Cost Allocation (Accounting);
  -- Performance Management;
  -- Fault Management;
  -- File System and Content Integrity Checks; and
  -- Media Management (e.g. Backup & Restore).

- Communication Management Services, including:
  -- State Management (e.g., Startup and Shutdown);
  -- User and Group Identification;
  -- Configuration Control;
  -- Service Access Control;
  -- Usage Management and Cost Allocation (Accounting);
  -- Performance Management;
  -- Fault Management; and
  -- Security Management.

5.4 Software Development Capabilities

Development of application software designed to operate as a part of a large scale distributed system will pose substantial new challenges. Successful application of the information infrastructure to application areas may require new software development technology and techniques to assure market success. In some sense the information infrastructure itself may be a key element in reducing costs, with the potential for a market economy for application software which may enable widespread software reuse and distribution. The capabilities required, based on those developed by the Navy Next Generation Computer Resources Program (NGCR)[12], include:

- Software Requirements Engineering Service - provides the capability to create and manipulate representations of requirements, including the ability to:
  -- capture and represent system requirements allocated to software elements;
  -- analyze system requirements allocated to software elements;
  -- refine and evolve system requirements allocated to software elements over time.

- Software Design Service - provides the capability to create a design of the software components of a system or subsystem., or modify such a design to conform to a new set of requirements.

- Software Generation Service - provides semi-automatic production of software using existing components or templates.

- Software Review and Modification Service - Prepare the source code of an application with a syntax-directed editor. This editor should have features such as the ability to:
  -- Find references to variables, routines, data structures, etc.;
  -- Check for syntax errors and assist the user in fixing those errors;
  -- Attach commentary to the source code that is not part of the source code.

- Software Simulation and Modeling Service - provides the ability to model (or prototype) a software design before full implementation takes place.

- Software Verification Service - provides the formal verification of software against its formal specifications for the purpose of locating errors.

- Software Compilation Service - Prepare the source code for an application, written in various programming languages, for execution on the application platform. This includes the ability to specify execution options where necessary. (On many systems, this is the traditional compilation and linking capability.)

- Software Static Analysis Service - provide for automatic or manually directed static examination of source code for software components and display of potential errors. This examination should support coding styles disciplines, including the ability to:
  -- Optionally enforce source code style rules;
  -- Reformat source code to conform to style rules;
  -- Handle multiple sets of stylistic rules.

- Software Debugging Service - support the location and repair of software errors in individual software components by controlled or monitored execution of the code. This support includes the ability to:
  -- run an application under complete control of a debugger, including tracing and the ability to examine program and data state;
  -- attach the debugging tool to an application while it is executing or after it has failed;
  -- produce a cross-reference listing of variables, routines, data structures, etc.

- Software Execution Efficiency Measurement Service - support the measurement of resource and time consumed in execution of a software component. Measurement should support accumulated time and resource consumed by multiple components:
  -- Routine or major block of code;
  -- Individual lines of code.

- Software Testing Service - support the testing of software systems, including the ability to:
  -- Generate test cases and test harness;
  -- Instrument source programs to output results;
  -- Test for resource utilization, reliability, path and domain selection;
  -- Perform timing analysis;
  -- Support regression testing; and
  -- Validate test results against expected results.

- Software Build Service - support the integration of separately developed software components into a single system. Automatically generate executable programs from multiple source code modules, including the ability to:

-- automatically determine which source code has been changed;
-- automatically determine the dependencies between source code modules;
-- generate previous versions of the software.

- Software Reverse Engineering - This service provides the capabilities needed to capture design information from source or object code and produce design documentation such as structure charts and call graphs.

- Software Traceability Service - support the recording of relationships between artifacts (including software components) of the software development process. Track revisions to these artifacts effectively including the ability to:
  -- check artifacts out for modification;
  -- check artifacts in after modification;
  -- determine the status of artifacts under development;
  -- query the modification history of artifacts;
  -- create complete revision history of all changes to artifacts.

6. The Profiling Process: Standards and Specification Selection

Organizations select the technical specifications to be used to satisfy their operational requirements. Engineering, procurement, and other organizational activities translate these operational requirements into technology requirements using processes that are generally too flexible, and difficult to codify. One result of these activities, however, is inevitably a set of technical specifications used as a basis for action by all involved parties. This set of specifications is a *profile*.

For a distributed system or infrastructure, this process is never completed. A standing process is required to maintain and update the set of profiles and specifications in use. Change may have many drivers. Service requirements change with the mission and structure of the organization. Sources of this organizational change are legion and well documented, and include competition (win, lose, or draw), leadership change, size (growth or shrinkage), and economics. New technology may trigger review to find new ways to accomplish tasks, and may be significant enough to affect the formulation of the organizations objectives (e.g., World Wide Web impact on group communications).

Whatever the source, a continuous stream of new requirements, technology, specifications and profiles will be considered by an actively evolving organization. This section outlines some of the concepts and criteria important in that specification selection and profiling process.

6.1 Types of Specifications and Selection Precedence

The identification of a complete, consistent suite of standards which addresses information infrastructure service requirements will, by necessity, draw from many sources. A brief discussion of the various types and sources is in order, since choices among these types may be required.

The specifications referred to in this discussion describe the technical function of technology. Besides the *functional specifications* referred to here, other specifications are required for pragmatic engineering and/or procurement. These additional specifications include performance, quality, reliability, etc. and not currently included in this document.

Standards are a special case, or type, of specification. They are specifications which have been through a formal ballot in a group open to wide participation, and have a known community of consensus. In the United States, there are a variety of voluntary standards organizations, each operating according to a wide variety of procedures, subject to basic ANSI guidelines. These groups produce formal, or *de jure standards*, which are considered U.S. *national standards*.

Other nations produce their national standards via a variety of methods which may vary greatly from the U.S. approach. U.S. and other national standards may progress to the international level, and undergo ballot. The scope of ballot may be regional (e.g., European, Pacific Rim, or North American) or global (e.g., ISO/IEC). A successfully balloted specification in the first case may be identified as a *regional standard*, and in the second case is labeled an *international standard*.

Users observe that increasingly there are specifications which provide needed and useful extensions to international standards, have broad consensus, and can meet user business needs in advance of the completion of the formal standards process. These specifications other than formal standards are necessary,

and a variety of these can become available by various means. Any specification which has established some consensus, but has not been formally balloted, is a *public specification*.

Often, a proprietary specification becomes widely adopted in the marketplace, by presenting a unique or overwhelmingly superior solution to a user need. The specification is often made available by the developer of the technology, sometimes in the public domain, sometimes on reasonable terms, in order to ensure widespread adoption. The specification may also become available when the intellectual property protection on the specification expires. These specifications which have been widely adopted as a result of marketplace success, but have not been through a consensus process are labeled as *de facto standards,* and are an important type of public specifications.

A variety of consortia or associations may offer users and providers faster and/or more directed opportunities to establish specifications. They are often oriented toward establishing a capability or technology in an environment where collaboration is important to share cost or achieve a critical mass (but not unanimous) consensus in the market. The specifications from these consortia are important and useful sources of concept and specification for users, but must be adopted carefully. Consortia are often established for competitive advantage, implying that there may be a rival source for competing teehnology or specifications. Selecting one competitor over the other may cause opposition from the losing side. Clear and equitable process is important in this situation. These organizations produce *consortia specifications*, another important type of public specifications.

Finally, there are specifications developed within an organization, where opportunity to participate and influence the specification is limited to those within the organization and invited guests. This may be appropriate, for instance, where there are truly unique requirements. These specifications are expensive since the developing organization must bear not only the cost of developing and maintaining the specification, but of developing compliant technology as well. Even if the technology is bought from an outside provider, the price will certainly reflect the full cost of development for unique technology. As an unintended side effect, use of these internal, or *private* specifications may make it difficult to make use of otherwise suitable commercially available technology which becomes available. This can effectively lock the organization into a dependency on the technology provider which can be very difficult and costly to reduce. A private specification protected by intellectual property restrictions which require an agreement prior to use of the specification, is a *proprietary specification*.

A precedence order is usually established by an organization in adopting specifications, to meet specific objectives. An organization may set a higher precedence for international standards, to meet international business objectives. Another organization may set a higher precedence on an application domain specification, to assure that unique requirements are met. As an example, the precedence order used for selection within POSIX 1003.0 [2] is as follows, in the order of most to least preferred:

1. Approved standards maintained by accredited international standards development organizations;
2. Approved standards developed by accredited regional bodies;
3. Approved standards developed by accredited national bodies;
4. Draft standards developed by accredited international bodies;
5. Draft standards developed by accredited regional bodies;
6. Draft standards developed by accredited national bodies;
7. Approved (as opposed to draft) specifications (widely adopted, but not formal standards) developed or maintained in an open forum; and
8. Specifications developed by a closed forum.

Note that the precedence begins with formal standards, which include the first four entries. The specifications listed in items five through eight are considered public specifications by the criteria in use in IEEE and ISO. The adherence to any precedence is not hard and fast, and should be considered as one more factor to be balanced in selecting specifications.

6.2 Selection Process

The process of selecting specifications could be structured to emphasize that specifications are selected to satisfy service requirements. The process may be summarized as follows:

- select from the set of international standards which satisfy the service requirements;
- where services are not satisfied, continue down the precedence hierarchy, selecting more specifications and satisfying further service requirements, until all levels of formal standards have been searched;
- begin selecting from available "public specifications" until all sources of public specifications have been evaluated;
- where standards are required, but not available from any source, develop a specification. The specification should be built on existing specifications and agreements where possible, with a minimum of invention.

6.3 Specification Selection Criteria

While no single set of guidelines is appropriate for all organizations, it is useful to collect and review criteria which have been found to be useful. The suggested criteria described below are offered as a starting point for organizations to adapt to their own needs. The following comments on the selection process and suggested selection criteria are based on those in IEEE 1003.0 "Guide to the POSIX OSE" [2], OSE Implementors Workshop procedures [13], ISO/IEC "Principles and Taxonomy for Open System Environment Profiles,"[14] and the NIST Application Portability Profile (APP)[15].

While it is clear that objective criteria are best, subjective measures are inevitable since intangible factors are important. Judgment is required to balance these criteria while selecting among candidate specifications, since many of the criteria fundamentally conflict.

These criteria can be applied to selection of both standards and public specifications. Where no candidate specification satisfies a service requirement, the unsatisfied requirements can be used to guide the modification of an existing specification which is a close fit, or the development of an entirely new specification.

Note that while the services are defined in section 4 "Service Definitions" with a clear partitioning in mind, existing specifications usually better reflect the charter of their parent organization. This effect (and the resulting difficulties) is amplified when multiple standards must be used together to create a profile. These standards were created within disparate organizations and projects, which were in many cases carried out in isolation from the others. As a result, mapping of services to standards is not simple. Flexibility and a strong measure of pragmatism will be necessary for success. Criteria which could be considered in selection of standards and specifications include:

- Service Requirements Addressed: A specification should be selected in response to specific service requirements. Standards and/or specifications selected may not align with the partitioning of services as outlined in section 4.

  As a general guideline, specifications which address more (or all) of the stated service requirements should be favored. Also, those specifications which have a more direct or clear relationship to those requirements should be favored.

- Stage of Development: Another factor involved in the selection of standards is "stage of completion." That is, there is a standards development life cycle process whose effects need to be taken into account. Most standards follow a sequence from approved development, through draft, and on to approved standard.

  As a general guideline, where choices are to be made among standards, standards which have progressed further through the process should be favored.

- Stability: This factor refers to anticipated change in the standard over time. This change may expand or contract the technical coverage of the standard.

  As a general guideline, the more stable standards are preferred over those subject to change. In some cases, however, stable standards should not be selected, as in the case of obsolete or un-implemented standards.

- Scope of Consensus: There are differences among standards development bodies with respect to their scope of consensus. Formal standards development bodies are typically chartered to develop standards for either international, regional or national communities. Other measures of scope or consensus are relevant as well. These measures of consensus could address consensus within relevant technical or commercial communities, for example.

  As a general guideline, standards with broader scope of consensus are preferred over standards with narrower scope of consensus scope of coverage. This results in a precedence for standards selection of international, followed by regional, followed by national body developed standards.

- Openness: Standards development organizations can differ from one another by virtue of their "openness." All standards bodies exhibit some legitimate barriers to participation. These may, for example, result from the need to provide equitable sharing of the cost of the forum. They could also be a side effect of maintaining a balance of constituencies represented in the membership, or limiting some aspects of participation at the international level to accredited delegations. The result is a varying degree of consensus in the technical content of the standards across development bodies.

  As a general guideline, standards developed by accredited standards development organizations (all of which use an open forum) are preferred over those standards developed by bodies using a closed forum.

- Consistency among Selected Specifications: Sets of standards, often called profiles, must be selected with some care to assure that those selected are consistent among themselves, i.e., do not contradict or conflict, or preclude the use of each other.

As a general guideline, specifications which may be used with a broader range of other specifications are preferred over those specifications which limit or preclude the use of other specifications.

- Availability for Unencumbered Implementation: Those specifications that may be used without encumbrance to implement conforming technology tend to achieve widespread use faster than specifications which have legal or financial constraints on their use. A specification qualifies as unencumbered even if the document itself is a salable item, as long as implementation of the specification carries no licensing fee.

  As a general guideline, specifications with fewer constraints on their widespread use and adoption are preferred over those specifications with more constraints.

- Product Availability: Specifications for which no (or very few) compliant products are available do not meet user's needs. The quality of available products is also a consideration, since this may affect the rate of adoption of the specifications.

  As a general guideline, specifications with more, higher quality compliant products currently in the marketplace are preferred over those specifications which have fewer.

- Maturity: Mature specifications have evolved through experience and use to be clearly defined, well understood and widely accepted, with a base of technical concept in widespread use.

  As a general guideline, more mature specifications are preferred over less mature specifications.

6.4 Considerations in Selection of Public Specifications

The Publicly Available Specifications should neither overlap with nor conflict with an existing formal standard or formal standard under development. That is, if a formal standard exists or is under development that provides the same function as the proposed Publicly Available Specifications, then the Publicly Available Specifications should be avoided, if possible. If a Publicly Available Specifications adds functionality to a standard, then it should be engineered to augment the formal standards in such a way that service requirements addressed by the formal standards are not adversely affected.

Where more than one Publicly Available Specification might serve as the basis for agreements for the same technical function, a rationale should be developed to record which of the several candidates should be used and under what circumstances. Users will make the final choice among competing Publicly Available Specifications in response to their specific requirements.

The criteria listed above apply to the selection of public specifications, as well as standards. Additional considerations in the selection of public specifications (known as Publicly Available Specifications in the workshop) are drawn from the OSE Implementors Workshop (OIW) procedures[13], and include:

- Common Description: The specification should be described using conventions, including conformance statements, appropriate for the existing formal standards which the specification augments.

- Stability: The specification will not change except as required to fix technical and editorial errors.

- Completeness: The specification must be sufficiently complete so as to allow useful and predictable implementation of the complete functionality from scratch.

- Proof of Concept: The specification has been demonstrated in at least one actual implementation to meet the user requirement in question.

- Reasonable Terms: The specification is available on terms consistent with copyright and patent guidelines of appropriate national and international standards communities.

7. Summary and Conclusion

A basis for definition of key services required to support information infrastructure activities includes the definition of an architectural framework. This approach identifies key entities, interfaces among the entities, and the services required, all in response to a set of objectives.

A set of objectives, entities, interfaces, and services is identified based on work in the Open Systems Environment community, produced in a variety of forums over the past seven years. There is evidence of substantial consensus and convergence on the technical concept described, that could be useful for further work on architectural frameworks for large-scale distributed systems.

Annex A:

Comparison of Information Technology Interfaces Identified in NII Related Documents

- Columns contain terms used by various groups to identify similar interfaces. See acronyms in notes below

Interface / Group or Document	Application Program Interface (API)	Information Service Interface	Human/Technology Interface	Communications Interface	Network to Network Interface	Application to Application Interface
IEEE P1003.0 "Guide to the POSIX Open System Environment"[2]	- Application Program Interface	- Information Service Interface EEI	- Human/Computer Interface EEI	- Communications Service Interface EEI	n/a	included as API, and treated as a service
Computer Systems Policy Project (CSPP)[7]	- Application to Appliance	n/a	n/a	- Application to Network	- Network to Network	n/a
Cross Industry Working Team (XIWT)[8]	- Application to Platform within an Information Appliance (2)	n/a	n/a	- Appliance to Network - ISP to Network (1)	- Network to Network	- ISP to ISP (1) - IA to IA (1) - ISP to IA (1)
ISO/IEC TSG-1 "Interfaces for Application Portability"[6]	- Application Program Interface	- Information Domain Service PEI(3)	- User Domain Services PEI(3)	- Communications Domain Services PEI(3)	n/a	n/a
NRC ODN Report[9]	n/a	n/a	n/a	- Open Data Network Bearer Service	n/a	n/a
"SPIRIT" rev. 1[16]	- Programming Interface	- Exchange Format Interface	- Human User Interface	- Protocol Interface	n/a	n/a

Notes:
(1) XIWT defines an Information Service Provider (ISP) and an Information Appliance (IA)
(2) XIWT describes "Portability" in terms of Appliance portability (or "mobility"), not application portability
(3) TSG-1 "Platform External Interface (PEI)" corresponds with 1003.0 "External Environment Interface (EEI)"

Annex B: References

References with an asterisk (*) after the reference number are listed as architectural framework documents in the table in Annex A

[1] Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," 15 September, 1993.

[2]* ISO/IEC TR 14252:1995 "Guide to the POSIX Open System Environment (OSE)," 1995. (Equivalent to IEEE 1003.0, in development since 1988.

[3] NIST Special Publication 857, "Putting the Information Infrastructure to Work," DOC, May 1994.

[4] NIST Special Publication 868, "The Information Infrastructure: Reaching Society's Goals," DOC, September 1994.

[5] Information Infrastructure Task Force, "R&D for the NII: Technical Challenges," Interuniversity Communications Council Inc., 1994.

[6]* ISO/IEC JTC1 N1335, "Final Report of ISO|IEC JTC1 TSG-1 on Standards necessary to Define Interfaces for Application Portability (IAP)," April 1991.

[7]* Computer Systems Policy Project (CSPP), "Perspectives on the National Information Infrastructure: Ensuring Interoperability," February 1994

[8]* Cross Industry Working Group (XIWT), "An Architectural Framework for the National Information Infrastructure," Corporation for National Research Initiatives, September 1994

[9]* National Research Council (NRC), "Realizing the Information Future - The Internet and Beyond," National Academy Press, June 1994 (also referred to as the Open Data Network, or ODN report.

[10] OSE Implementors Workshop, "Requirements for Distributed Systems Management," Distributed Systems Management Working Group, January 1995

[11] ISO/IEC IS 10032:1995(E), "Reference Model of Data Management," 1995. Addresses a scope similar to Information Management Services described here, but significantly broader.

[12] NIST Special Publication 500-213, "Next Generation Computer Resources: Reference Model for Project Support Environments (Version 2.0)," DOC, November 1993

[13] NIST Special Publication 500-224, "OSE Implementors Workshop Stable Document Part 1-Workshop Policies and Procedures," DOC, 1993

[14] ISO/IEC JTC1 TR10000-3: 1995, "Information Technology - Framework Taxonomy of International Standardized Profiles - Part 3: Principles and Taxonomy for Open System Environment Profiles"

[15] NIST Special Publication 500-210, "Application Portability Profile: The US Governments Guide to the Open System Environment (Version 2)," DOC, June 93.

[16]* Network Management Forum, "Service Providers Integrated Requirements for Information Technology," Issue 1 (or "SPIRIT"), September 93

☆U.S. GOVERNMENT PRINTING OFFICE: 1996 - 404-525/47917

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500–.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899–0001