**Network and Services
Integration Forum**

NSIF-036-2000

(NSIF Document NSIF-DN-9706-045R6)

NSIF APPROVED DOCUMENT

WORK GROUP: Distributed Network Management Environment (DNME)

TITLE: CIT/OS Software Platform Architecture

DATE: December 1, 1999

EDITOR: **Name:** **Connie Hunt**
Voice: **314-235-0260**
email: **ch9578@momail.sbc.com**

ABSTRACT:

The Distributed Network Management Environment (DNME) subgroup and the former CIT/OS Common Platform subgroup have produced requirements and architecture specifications that depend on the definition of open software platforms for Operations Systems and Craft Interface Terminals. This document serves as an umbrella document that describes the platform architectures for OSs and CITs conforming to one or more of these and other specifications. Detailed descriptions of individual platform components, and their associated APIs, are covered elsewhere.

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

TABLE OF CONTENTS

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

1. Introduction

This document was created by the SONET Interoperability Forum to provide a roadmap for both OS and CIT software platform definition and to provide a foundation for a variety of applications addressed by the SIF. With the evolution of SIF into the Network and Services Integration Forum, it was decided to conclude this work and focus on other areas. This document has been finalized and will serve as an overview of the completed software platform work. In the future NSIF may decide to address other components of this work.

As an umbrella document it references other detailed SIF specifications for individual platform components and summarizes platform requirements at a high-level. Since many of the services needed on OSs and CITs are the same (e.g., name/address resolution, security) the intent is to capture as much commonality as possible across both platforms, while making clear differences where they exist.

This common foundation will enable service providers to have greater freedom in choosing hardware and software from different vendors without having to worry about incompatibilities in platform and without incurring large porting costs. It will free providers of platform software to focus on enhanced tools and services instead of supporting many flavors of platform infrastructure. This in turn will enable companies providing management applications to support their products on a variety of hardware platforms with reduced expense, and rely on commonly available platform services to reduce development time.

1.1 Acronyms and Abbreviations

ACSE   Association Control Service Element

API   Application Programming Interface

ASE   Application Service Element

CIT   Craft Interface Terminal

CMISE   Common Management Information Service Element

FTAM   File Transfer & Access Management

LDAP API   Lightweight Directory Access Protocol API

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

NARSE   Name Address Resolution Service Element

NE   Network Element

OS   Operations System

OSI   Open Systems Interconnection

TARP   TID Address Resolution Protocol

TL1   Transaction Language 1

XAP API   X/Open ACSE/Presentation services API

2.   Generic Platform Requirements

There are several concerns and issues around defining a successful multi-vendor platform that may impact vendors that supply platform components, applications that interact with these components, and service providers responsible for system integration. An initial set of generic requirements for CIT and OS hosts are:

- Use of industry standard APIs

- Dynamic linking of modules

- Multi-threading

- Support for multiple operating systems (UNIX flavors and WindowsNT[1])

Dynamic Library Naming Rules for use with CIT/OS Applications [9] defines a set of rules to improve the resiliency and the cross-vendor portability of CIT/OS applications built on top of SIF approved APIs. It deals with particular issues related to dynamic linking, a method for sharing modules among processes and loading/unloading them at the application's convenience. It provides conventions for WindowsNT[1] and three UNIX operating systems.
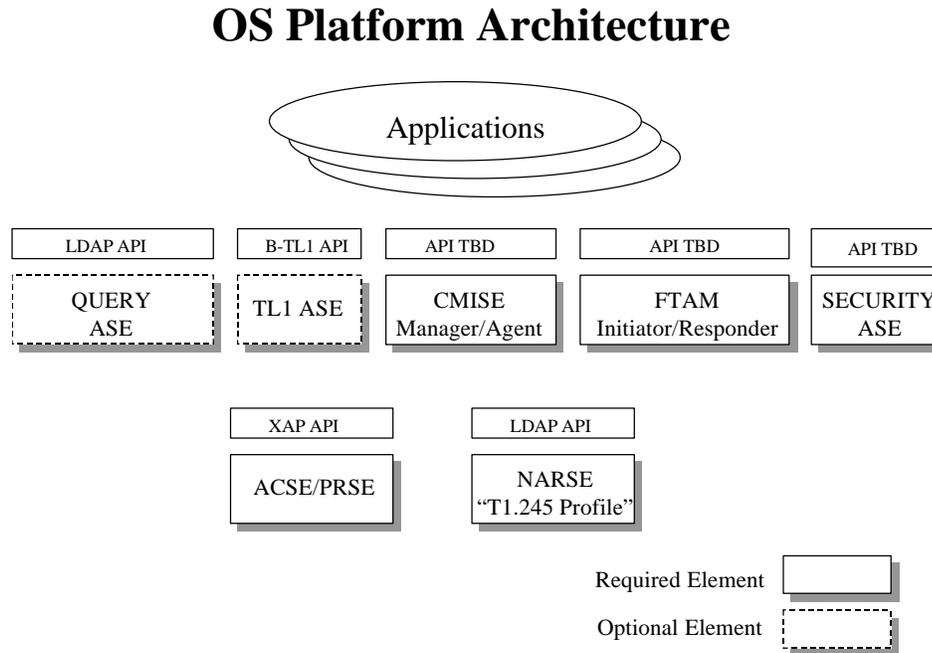
---

[1] Windows NT is a registered trademarks of Microsoft Co.

This document has received the approval of the Network Services and Integration Forum (NSIF).

3.   OS Platform Architecture

The SIF has produced requirements for OS platforms [1] which include mandatory CMISE, FTAM, security and T1.245 elements. The OS platform architecture depicted below has been chosen to satisfy these requirements.

OS Platform Architecture

Applications

LDAP API	B-TL1 API	API TBD	API TBD	API TBD
QUERY ASE	TL1 ASE	CMISE Manager/Agent	FTAM Initiator/Responder	SECURITY ASE

XAP API	LDAP API
ACSE/PRSE	NARSE "T1.245 Profile"

Required Element

Optional Element

UNIX is the preferred operating system for the OS platform. Use of the Microsoft WindowsNT[1] operating system is optional.

4.   CIT Platform Architecture

To date the primary SIF requirements specification driving CIT platform definition has been the SIF NE-NE Remote Login Implementation Specification [2], which requires a CIT to incorporate an open software platform providing OSI stack services. The remote login requirements also stipulate the use of the Microsoft Windows NT operating system to facilitate the ability of vendors supplying platform components and vendors supplying application specific software using these components to integrate their products on a single CIT.

---

[1] Windows NT is a registered trademarks of Microsoft Co.

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

The figure below shows the block architecture for a CIT software platform that can be used to support SIF multi-vendor remote login, and, potentially, other applications addressed by the SIF. This CIT platform currently has two required components, ACSE/Presentation Data Service and NARSE ("core" profile), plus several optional components. As an example of how a minimal platform with just the two required components might work, security, normally present in a more robust implementation, might be provided at the application level.

CIT Platform Architecture
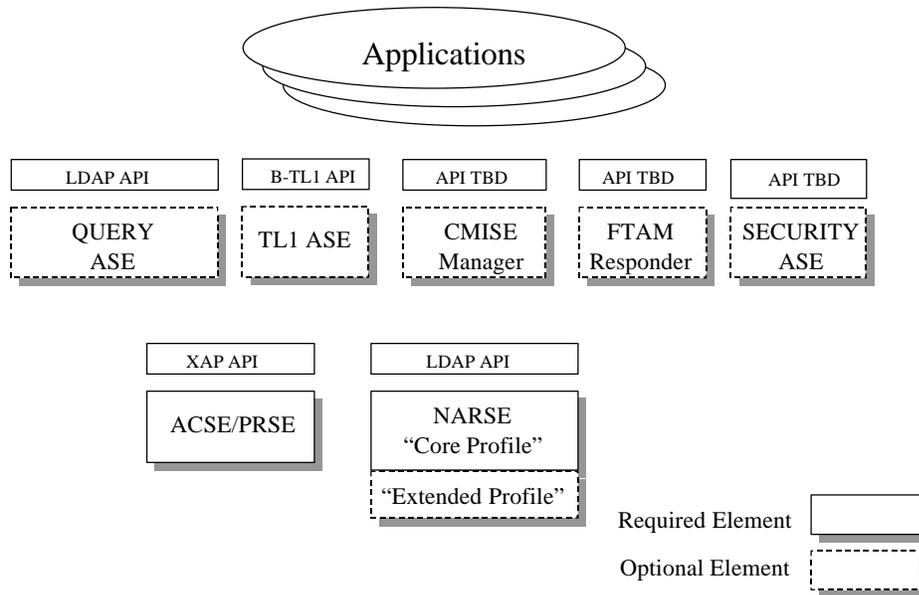
5.   Platform Component Descriptions

This section gives high-level descriptions of the components found on the CIT/OS platforms. An individual component may apply to both platforms, or just the OS or CIT.

5.1   ACSE/Presentation Data Service

The Association Control Service Element (ACSE) / Presentation Data Service component provides basic OSI association management and data presentation services. Applications or other platform components may obtain these services using the XAP API. A detailed description of this component and its XAP profile is provided in "SIF Profiling XAP for CIT/OS Systems" [4].

5.1.1   OS Platform

The ACSE/Presentation Data Service component is mandatory for an OS.

5.1.2 CIT Platform

The ACSE/Presentation Data Service component is mandatory for a CIT.

5.2 NARSE

The Name Address Resolution Service Element (NARSE) is used to satisfy application requests for name/address resolution services which may be rendered using TARP, T1.245 Directory Services, or locally configured information. A detailed description of this component is provided in "Network Address Resolution and Query Services for CIT/OS Systems" [5]. Applications or other platform components may obtain name address resolution services using the LDAP API and the unified schema that this API provides. LDAP schema definitions are provided in "Lightweight Directory Access Protocol: ANSI T1.245 and SIF Schema Definitions" [6].

Multiple NARSE variations and their corresponding LDAP profiles are defined in [5]. Two levels of service are possible: core and extended. The second dimension is how a given service is provided (TARP, T1.245 Directory Services, or locally local database). The particular NARSE requirements for each platform are identified below.

5.2.1 OS Platform

For an OS the "extended" profile (R2 in [5]) is mandatory, with T1.245 support (R3) only.

5.2.2 CIT Platform

For a CIT the "core" profile (R1) is mandatory with both T1.245 (R3) and TARP (R4) support. The "extended" profile (R2) is optional.

5.3 QUERY SE

The intent of this service element is to provide a generic query capability for a TMN directory (X.500-based) or local database. A detailed description of this component is provided in "Network Address Resolution and Query Services for CIT/OS Systems" [5]. This service element is a superset of the NARSE. The NARSE, however, is specific to name/address resolution.

5.3.1 OS Platform

The Query profile is optional for an OS.

5.3.2 CIT Platform

The Query profile is optional for a CIT.

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

5.4 TL1 ASE

The purpose of this component is to provide an operating system independent low-level API for TL1 applications, insulating the application from the underlying communication network. Low Level TL1 API [8] defines a specification for a Basic TL1 API (BTL1 API). It also defines a specification for a BTL1 Library for a possible implementation of a library providing the BTL1 API service to application programmers.

5.4.1 OS Platform

A TL1 component is optional for an OS.

5.4.2 CIT Platform

A TL1 component is optional for a CIT.

5.5 CMISE

The TeleManagement Forum TMN C++ API and specification for underlying CMISE services is an industry standard API that could be used on OS platforms. A profile is needed and is possible future work.

5.5.1 OS Platform

CMISE manager/agent components are required for an OS.

5.5.2 CIT Platform

CMISE agent and manager components are optional for a CIT.

5.6 FTAM

The document SIF-011-1997, *SONET Operations Communications FTAM Profile,* provides a profile for FTAM implementation. This document assumes that profile is employed and shows an FTAM API. Definition of a standard API has not been done and is possible future work.

The OS platform and CIT platform are discussed below and three examples are given to illustrate when the Initiator and Responder roles are appropriate.

5.6.1 OS Platform

FTAM Initiator and/or Responder components are required for an OS platform when that OS needs to transfer files to and from another OS or NE. When the OS maintains a file store and

---

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

needs to upload and download files from an NE or other OS, then the OS is required to support the Responder role. When the OS needs to transfer to or receive files from another OS which is operating as an FTAM Responder, it needs to support the FTAM Initiator role.

Following are two examples of OSs supporting FTAM Initiator or Responder roles:

1. *The OS is providing Software Management services to NEs*. As defined by Bellcore GR-1250 [6], new software generics for the NEs are stored on the OS; the download of the software to an NE and the installation of the software on the NE is managed by the OS. Files may be created to store an NE's provisioning and saved on the OS to be used to restore that NE in case of a failure. In these cases, the OS needs to support the FTAM Responder role.

2. The OS is using electronic bonding to exchange billing data with another OS responsible for maintaining billing records. When FTAM is used for this purpose, the OS sending data needs to support the FTAM Initiator role and the receiving OS needs to support the FTAM Responder role.

5.6.2   CIT Platform

An FTAM Responder component is optional for a CIT when it is used to store files that are being received from and/or sent to the NE as in the examples above. The CIT may also function as an FTAM Initiator when it is interacting with an FTAM Responder on a higher level OS.

The following example illustrates when the Initiator role might apply for the CIT:

The CIT retrieves from an FTAM Responder a file of provisioned parameters to be used in restoring an NE that has lost communications to higher level OSs.

5.7   Security ASE

Requirements for SIF OS Platforms [1] specifies that CMISE communications be authenticated at association set up time using the ACSE Authentication Functional Unit. If data security is required, mechanisms described in T1.259, STASE-ROSE may be used.

Definition of a standard API has not been done and is possible future work.

5.7.1   OS Platform

A Security component is required for an OS supporting CMISE communications.

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000

5.7.2 CIT Platform

Security components are optional for a CIT.

6. References

1) "Requirements for SIF OS Platforms", SIF-016-1997, SONET Interoperability Forum, December 101997.

2) "NE-NE Remote Login Implementation Requirements Specification", SIF-009-1997, SONET Interoperability Forum, February 13, 1997.

3) "Remote Login Implementation Requirements Specification", SIF-002-1996, SONET Interoperability Forum, April 26, 1996.

4) "Profiling XAP for OS/CIT Systems", SIF-012-1997, SONET Interoperability Forum, August 28, 1997.

5) "Network Address Resolution and Query Services for CIT/OS Systems", NSIF-035-2000, Network and Services Integration Forum, November 5, 1999.

6) "Lightweight Directory Access Protocol: ANSI T1.245 and SIF Schema Definitions", SIF-015-1997, SONET Interoperability Forum, August 26, 1997.

7) "Generic Requirements for Synchronous Optical Network (SONET) File Transfer", GR-1250, Bellcore, June 1995.

8) "Low Level TL1 API", NSIF-030-1999, SONET Interoperability Forum, November 10, 1998.

9) "Dynamic Library Naming Rules for use with CIT/OS Applications", SIF-017-1998, SONET Interoperability Forum, April 20, 1998.

This document has received the approval of the Network Services and Integration Forum (NSIF).

February 10, 2000