Network and Services Integration Forum

APPROVED DOCUMENT

Network and Services Integration Forum

WORK GROUP:	**NSIF**
TITLE:	**Security Requirements for Operations Interfaces in a Multi-technology Network**
DATE:	**August 23, 2001**
EDITOR:	**Name: Connie Hunt – SBC Communications** **Voice: 314-235-0260** **email:** ch9578@momail.sbc.com
CONTRIBUTORS:	**Connie Hunt (SBC)** **Ron Roman (Telcordia)** **Kenneth Stephens (BellSouth)**

ABSTRACT: This document identifies security methods that can be used to secure NE and OS operations interfaces for the set of network technologies of interest to NSIF members. An attempt was made to select **common security methods** that could be used with the communications protocols that are within the scope of this document. SSL3 was chosen as the common security method for TCP/IP based communications..

Table of Contents

Security Requirements for Operations Interfaces in a Multi-technology Network

1 Introduction and Purpose

Carrier competition, increasing network capacities, and the acceleration of new network technology introduction and change, have made network reliability and integrity a business necessity for Network Providers. As network operations have progressed with the implementation of LAN access to NEs and use of standard published interfaces, there is a concern that there is more opportunity for unauthorized access to NEs and Operations Support Systems. These concerns are motivating Network Providers to look for ways to improve the security of their network operations, while minimizing the security administration aspects.

This document identifies security methods that can be used to secure NE and OS operations interfaces for the set of network technologies that are described in NSIF-039-2000, *NSIF Reference Architectures*. Security standards and documents from T1M1.5, the ATM Forum and the Internet Engineering Task Force (IETF), as well as earlier NSIF and SONET Interoperability Forum (SIF) security work, were reviewed for applicability to this effort.

An attempt was made to select **common security methods** that could be used with the communications protocols that are within the scope of this document. Using consistent methods across all operations interfaces has the potential to reduce administration and security infrastructure costs, increase the likelihood of interoperability, and speed the deployment of security implementations.

2 Scope

The scope of this document is security requirements for network management interfaces. The security features that are to be supported by the management interfaces are defined in Section 4. The solutions proposed in this document are focused on public key technology, and more specifically on Secure Socket Layer Protocol Version 3.0 (SSL3). Sections 5 and 6 give more information on these.

When developing this document, the contributors had management of transport network technologies in mind, such as SONET and Dense Wavelength Division Multiplexing (DWDM), but the security methods should be applicable to management of other wireline network technologies as well. See NSIF-039-2000, *NSIF Reference Architectures*, for examples of multi-technology networks. Across these multi-technology networks there are some variations in the preferred communications protocols for network management. Section 7 identifies the protocols that are of most interest, and Section 8 defines their security requirements.

The following sub-section identifies the network management interfaces that are within the scope of this document.

2.1 Reference Model

The areas of focus for the NSIF security work in relationship to the Telecommunication Management Network (TMN) Architecture is shown in Figure 1. ITU-T Recommendation M.3010, *Principles for a Telecommunication Management Network*, has three architectural perspectives. The components of the functional architecture shown in this diagram are:

1. The three principle function blocks –
    - the Operations System Function block (OSF)
    - the Network Element Function block (NEF), which is only partly within the TMN Architecture
    - and the Workstation Function block (WSF)
2. The reference points -q, x and f
3. The five logical layers –
    - Network Element Layer (NEL)
    - Element Management Layer (EML)
    - Network Management Layer (NML)
    - Service Management Layer (SML)
    - Business Management Layer (BML)

The components and their relationship to one another create a logical model and are not meant to represent any physical implementation. For example, EML functions may be deployed within an NE, or an NMS may communicate directly with an NE. The x reference point, which represents a potential interface between two TMNs, (e.g. two carriers), may be present at any OSF layer. For example it can be present between the EML in one TMN and the NML in the second TMN.

As noted previously, the x reference point represents potential interfaces between two TMNs. The q reference point represents potential interfaces between an OSF and an NE, and between OSFs that are internal to a TMN. The f reference point represents potential interfaces between OSFs and WSFs. NSIF security work is focused on the q and f reference points that will be implemented as interfaces at the bottom three layers: the NEL, EML and NML.

The Craft Interface Terminal Function block (CITF), shown in the Network Element Layer, is not a TMN architecture component. Since a WSF can only relate to an OSF, and not an NEF, the CIT does not fit the WSF definition, and is outside of the TMN domain. Since the CIT is an important security consideration for NSIF, the CITF has been added to the diagram to show that the CIT is within the NSIF security work scope.

Network Providers may offer a service to their customers, which provides management functions for some components of the customers' networks. The TMN Architecture also doesn't address this relationship. An interface line is shown in Figure 1 between the Network Provider OSF and the

Customer NEF to represent this case.

The large shaded area in the diagram shows the NSIF area of focus for security work.

The next section, which provides some scenarios, gives more information on what interfaces are recommended.

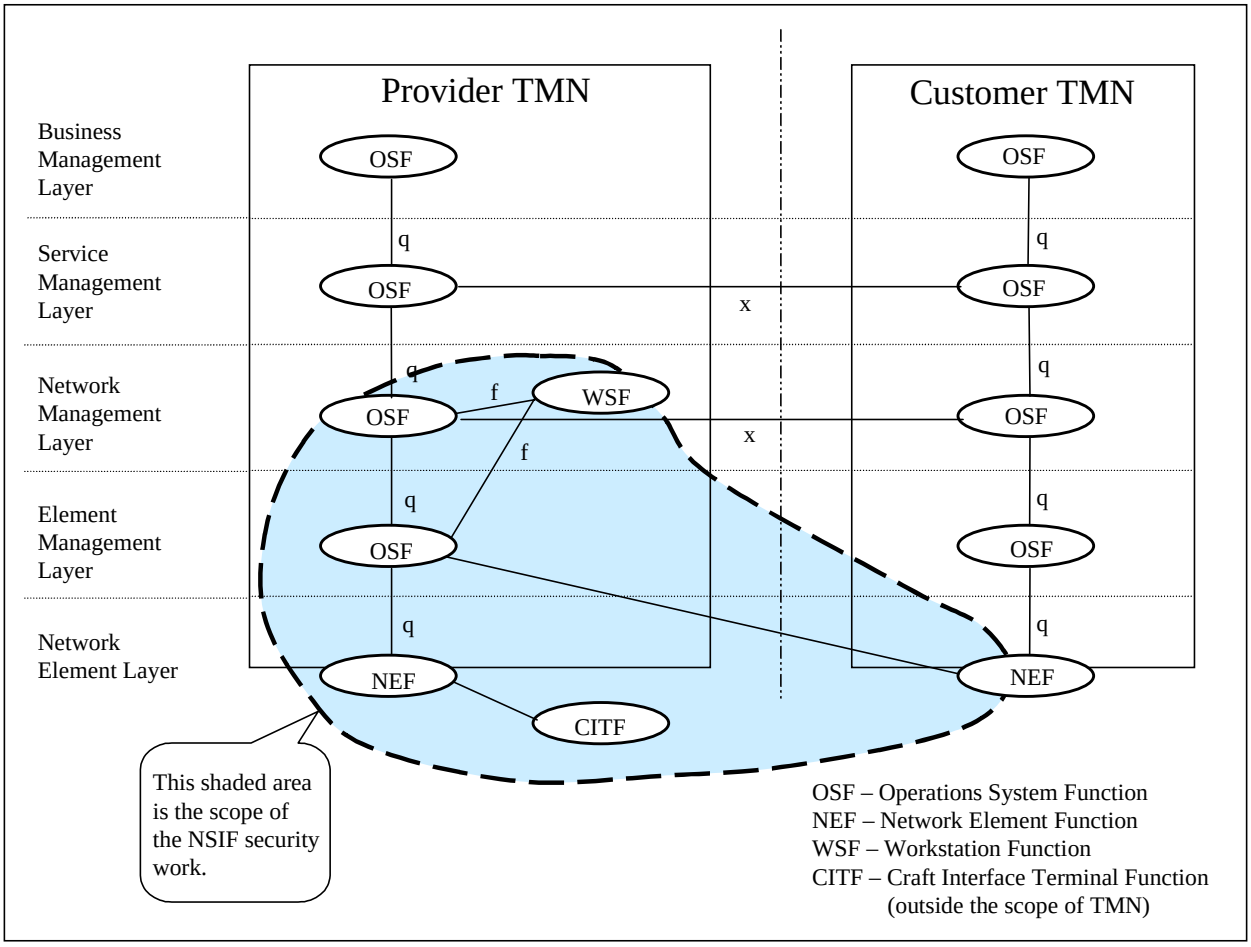

Figure 1 – Scope of NSIF security work in relation to the TMN Reference Model

3 Access Policy Scenarios

The scenarios shown in this section depict access policies that Network Providers have established for network management. Policies may vary among Network Providers, but these are believed to be most typical. They are provided in this document to demonstrate what kinds of interfaces are used in managing the Network, and consequently, will need to have security requirements defined. DWDM and SONET elements are shown as an example in the scenarios, but these policies should also be applicable to other transport elements that are within the NSIF scope.

The diagrams used in the scenarios are simplified and are not meant to represent a real deployment. They show the access points within a Network Provider administrative domain (or TMN), and between the Network Provider domain and the Customer Domain. The Customer Domain area represents a second TMN, which could be a business customer, or another Service Provider or Network Provider, such as an inter-exchange carrier, competitive local exchange carrier (CLEC), Internet Service Provider (ISP), etc. The dotted line in the middle represents the boundary between the two administrative domains.

The Network Provider has a set of Operations Systems (OSs) for managing their networks. These may consist of Element Management Systems (EMSs), Network Management Systems, Service Management Systems (SMSs) or legacy Operations Systems. These systems are represented in the diagrams as a box labeled “OS” with bubbles for the possible TMN layers that may exist. The customer may also have a set of OSs.

In each scenario diagram, the access point (or interface) of interest to the NSIF security work is marked with an arrow. The **Recommended** and **Not Recommended** labels that are used in the following scenarios indicate the Network Provider’s policy in respect to the described scenario.

In the following sub-sections, Scenarios 1, 2 and 3 pertain to internal network management by the Network Provider, Scenarios 4, 5 and 6 pertain to Customer Network Management (CNM), and Scenarios 7 and 8 pertain to the Network Provider managing the customer’s network.

3.1 Scenario 1 – Customer Services over Metro DWDM/SONET Rings Managed by Network Provider

The services offered by Network Providers over their networks, such as T1 services, are managed by the Network Provider's Operations Systems (OSs). Some of the management is fully automated and some of it requires manual intervention via user workstations. The customer has no access to the NEs for management purposes or access to the Network Provider's management systems.

It is recommended that all remote access to the Network Provider's NEs shall be from the Network Provider's OSs.

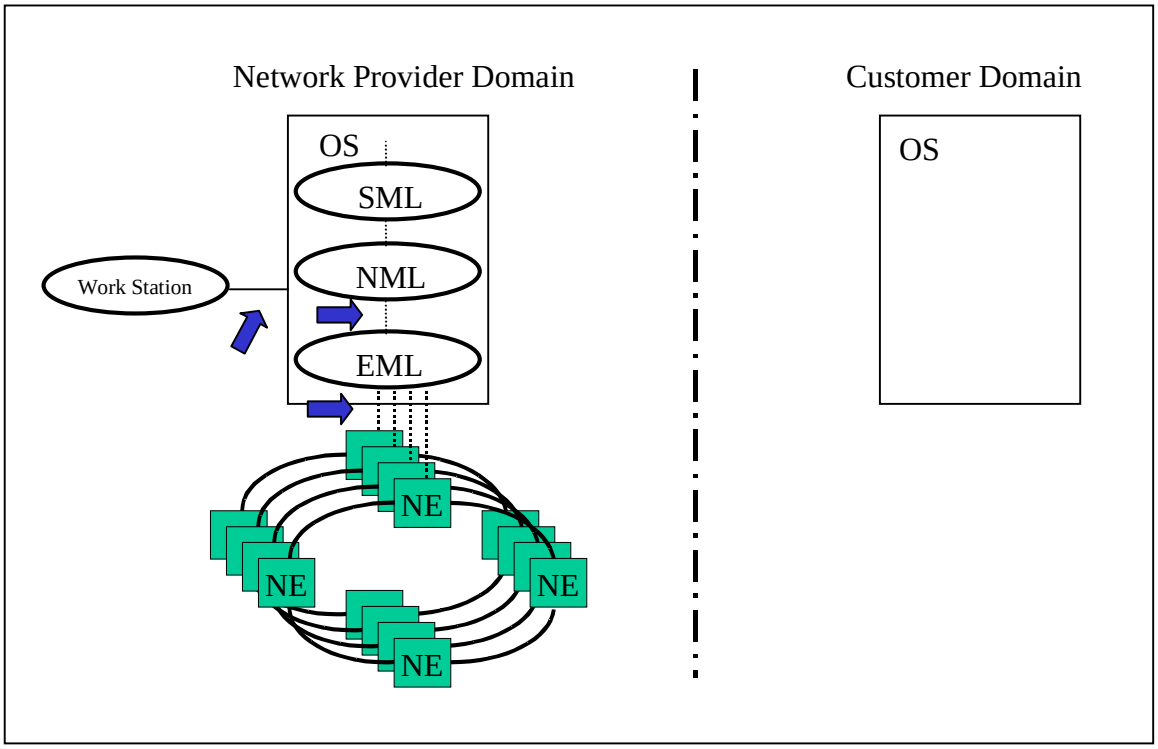

Figure 2 - Scenario 1: Customer Services over Metro DWDM/SONET Rings Managed by Network Provider

3.2 Scenario 2 – Customer Leased Metro DWDM/SONET Rings Managed by Network Provider

The majority of customer leased subnetworks offered by Network Providers are managed by the Network Provider's OSs. This scenario is the same as Scenario 1 except that the services (NEs or rings) are dedicated to a particular customer.

It is recommended that all remote access to the Network Provider's NEs shall be from the Network Provider's OSs.

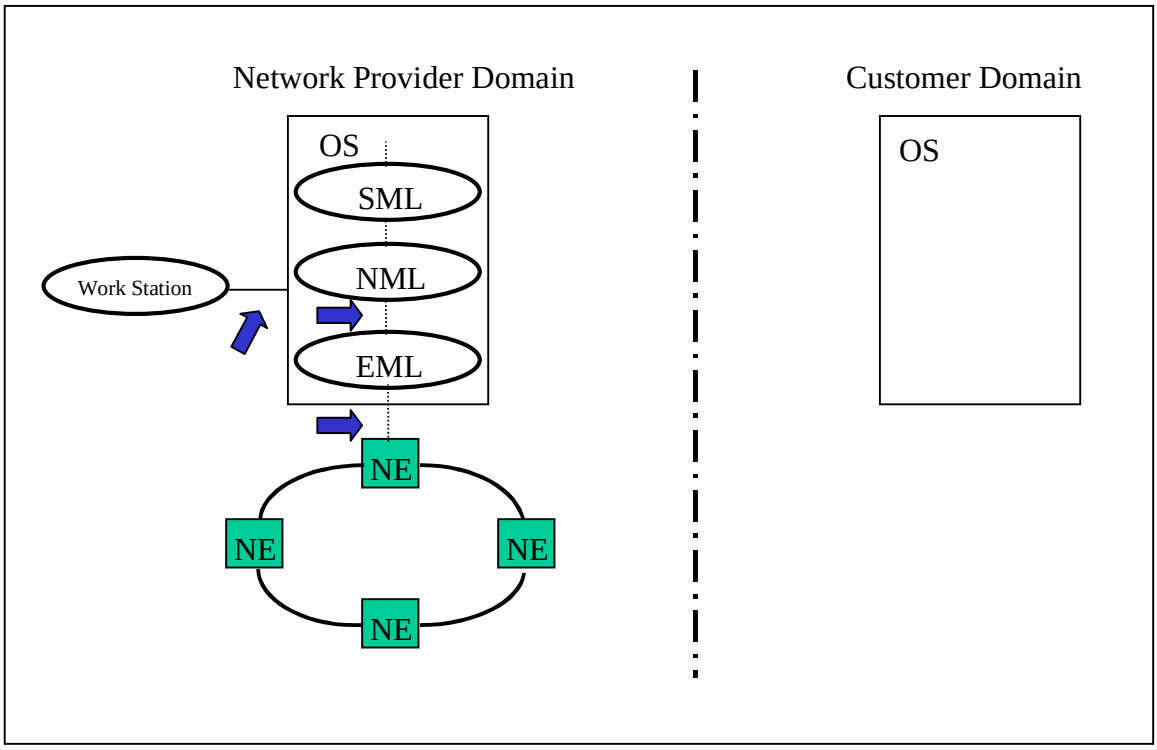

Figure 3 – Scenario 2: Customer Leased Metro DWDM/SONET Rings Managed by Network Provider

3.3 Scenario 3 – Local Craft Interface Terminal (CIT) Access to DWDM/SONET Rings

On occasion, the Network Provider will require access to NEs via a local craft interface terminal (CIT) to perform repairs and maintenance. If the NE does not support public key technology, this access should only be used when absolutely necessary since it requires that the NE's security information be updated with the CIT user's ID and password. It is preferred that access to the NEs be done through the Network Provider's OS's or through a security server as described in NSIF-038-2000, *NSIF Requirements for a Centralized Security Server*, whenever possible.

It is recommended that CIT access to NEs be limited to those cases where local access in necessary.

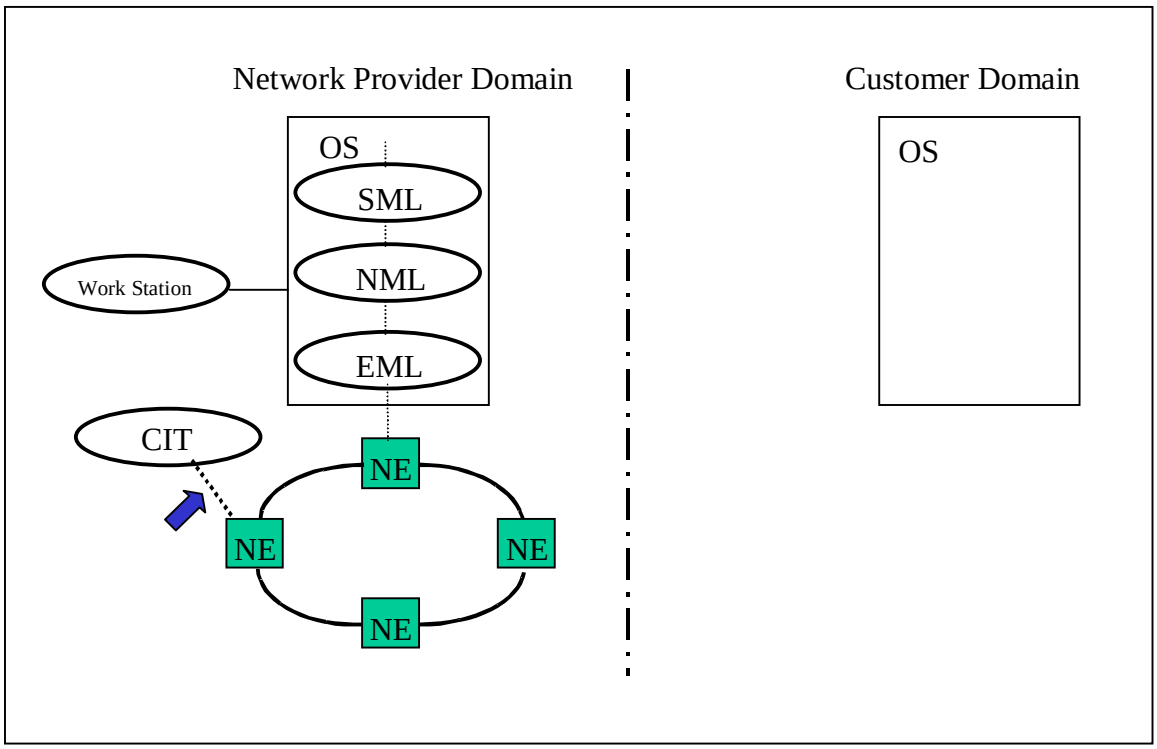

Figure 4 – Scenario 3: Local Craft Interface Terminal (CIT) Access to DWDM/SONET Rings

3.4 Scenario 4 – Customer Leased Metro DWDM/SONET Rings Managed by Direct Customer Access

This Scenario provides for the customer to have network management capabilities, which may be called Customer Network Management (CNM) service. Unless the customer leased ring is completely isolated from the rest of the Network Provider's network (e.g., no Data Communication Channel (DCC) or Optical Supervisory Channel (OSC) connection is enabled), allowing a Customer direct access to the NEs could provide the Customer with access to other Network Provider NEs.

It is not recommended to allow customer access directly to the Network Provider's NEs.

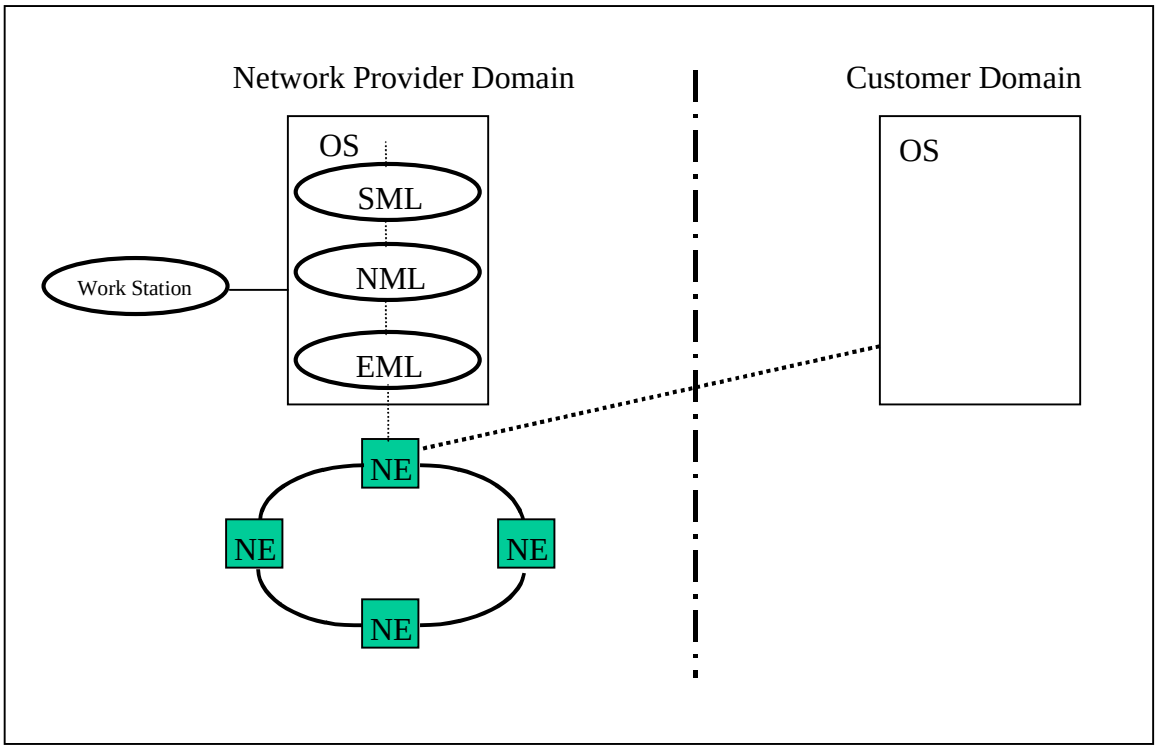

Figure 5 – Scenario 4: Customer Leased Metro DWDM/SONET Ring managed by Direct Customer Access

3.5 Scenario 5 – Customer Leased Metro DWDM/SONET Rings Managed by Indirect Customer Access

This Scenario provides the customer with CNM capabilities by offering these services through the Network Provider's OS. Requiring the customer to access the NEs through the Provider's OS allows the Provider to restrict access only to the NEs that the customer is leasing without blocking the DCC or OSC. In addition, this controlled access could also allow the Provider to restrict the commands available to the customer, if required.

It is recommended that any customer access to Network Provider network management capabilities be through the Network Provider's OSs. This scenario depicts existing or potential TMN X interfaces. These interfaces are currently **not within the scope** of NSIF work and are not addressed in this document.

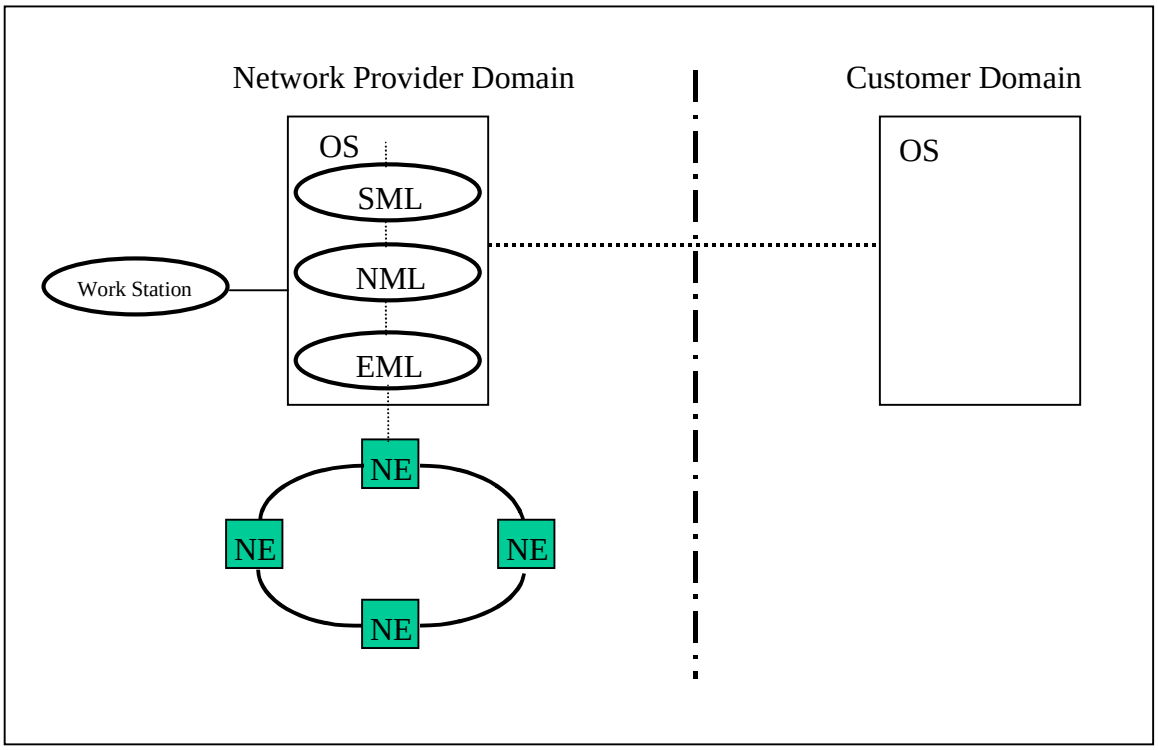

Figure 6 – Scenario 5: Customer Leased Metro DWDM/SONET Ring Managed by Indirect Customer Access

3.6 Scenario 6 – Network Provider Metro DWDM/SONET Rings Managed by Indirect Customer Workstation Access

This Scenario provides the customer with CNM capabilities by using a workstation to access the Network Provider's OSs. The access may be to the same OSs that the Network Provider uses to manage its network or it may be to a separate system, such as a CNM application web server that is created for this purpose. In either case, security features are required to limit customers from only accessing data and functions that pertain to their services.

It is recommended that any customer access, including workstation access, to Network Provider network management capabilities be through the Network Provider's OSs. This scenario is another variation of Scenario 5, which depicts a TMN X interface between the Network Provider's OS and the Customer's OS. This type of access is also **outside the scope** of this document.

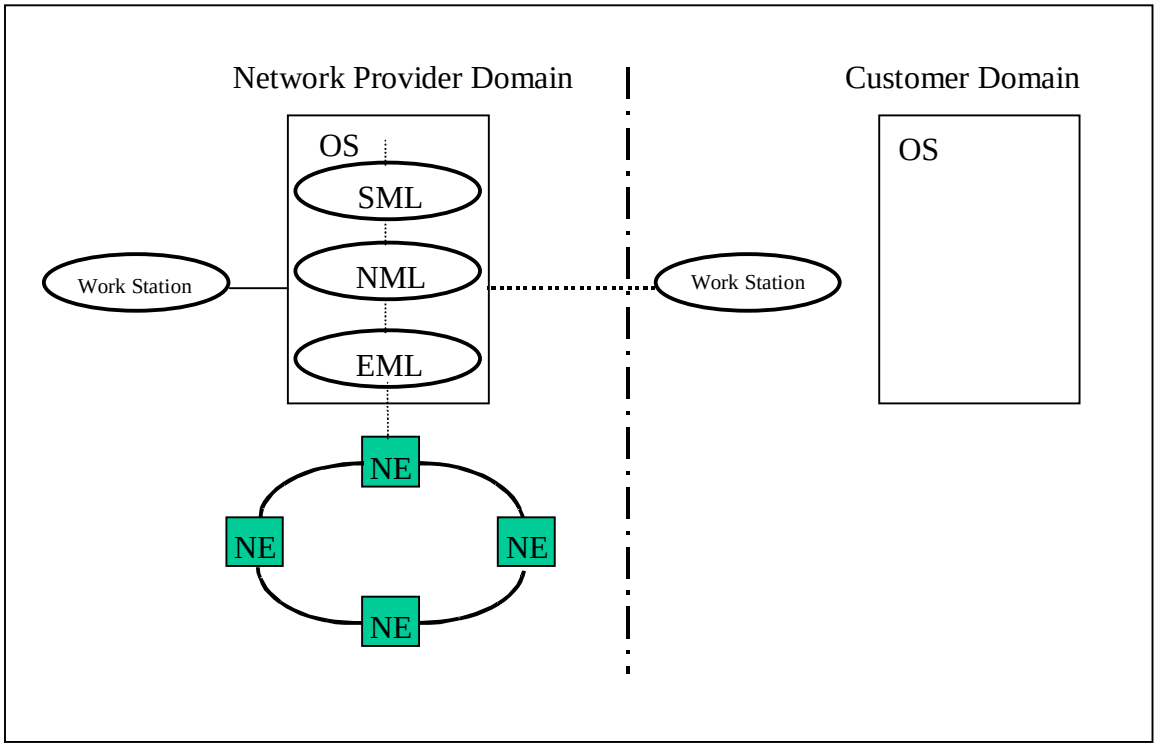

Figure 7 – Scenario 6: Network Provider Metro DWDM/SONET Rings Managed by Indirect Customer Workstation Access

3.7 Scenario 7 – Customer NEs Managed by Indirect Network Provider Access via DCC/OSC

The Network Provider may offer a service where the Provider manages the Customer-owned NEs. Access to the customer NEs using the DCC/OSC could provide an undesired impact to both the Provider and customer's networks. The additional administrative problems with this access make it very difficult to manage for both the Provider and the customer.

For the SONET case, SIF-010-1998, *Intercarrier Interface Recommendations*, states that the intercarrier use of the DCC is prohibited. SIF-010-1998 also discusses the need to propagate SONET overhead bytes across the intercarrier interface.

For the DWDM case, it is recommended that NSIF perform a similar study to what was done for SONET in producing the SIF-010-1998 document. For the purposes of this document, it is assumed that such a study would yield a similar recommendation to that produced for SONET. However, additional study is needed since this assumption may not turn out to be true, particularly in light of emerging industry proposals on the definition of the OSC, the transport of Automatic Switched Transport Services (ASTN) control plane applications, and Public Key Infrastructure (PKI) security standards.

It is not recommended that the Network Provider access customer NEs via the DCC or OSC for management purposes.

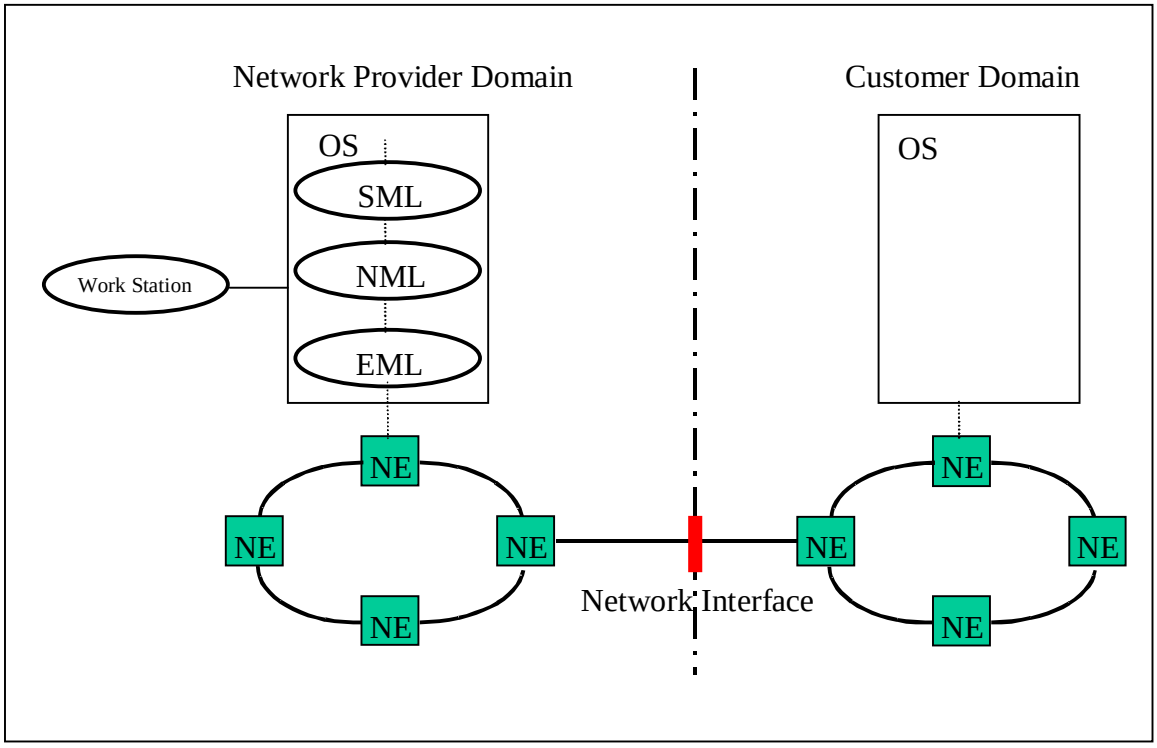

Figure 8 – Scenario 7: Customer NEs Managed by Indirect Network Provider Access via DCC/OSC

3.8 Scenario 8 – Customer NEs Managed by Network Provider OS Access

As in Scenario 5, the Network Provider may offer a service where the Provider manages the customer-owned NEs. This may be done with the Provider's OSs or with special OSs for this purpose. Figure 9 shows an interface between the Network Provider's OS and the customer's NE for the purpose of managing the customer's network. The DCC or OSC between the domains at the Network Interface is not enabled.

It is recommended that the Network Provider access customer NEs directly via an OS interface for management purposes.

For the SONET case, SIF-010-1998, *Intercarrier Interface Recommendations*, states that the intercarrier use of the DCC is prohibited. SIF-010-1998 also discusses the need to propagate SONET overhead bytes across the intercarrier interface.

For the DWDM case, it is recommended that NSIF perform a similar study to what was done for SONET in producing the SIF-010-1998 document. For the purposes of this document, it is assumed that such a study would yield a similar recommendation to that produced for SONET. However, additional study is needed since this assumption may not turn out to be true, particularly in light of emerging industry proposals on the definition of the OSC, the transport of Automatic Switched Transport Services (ASTN) control plane applications, and Public Key Infrastructure (PKI) security standards.

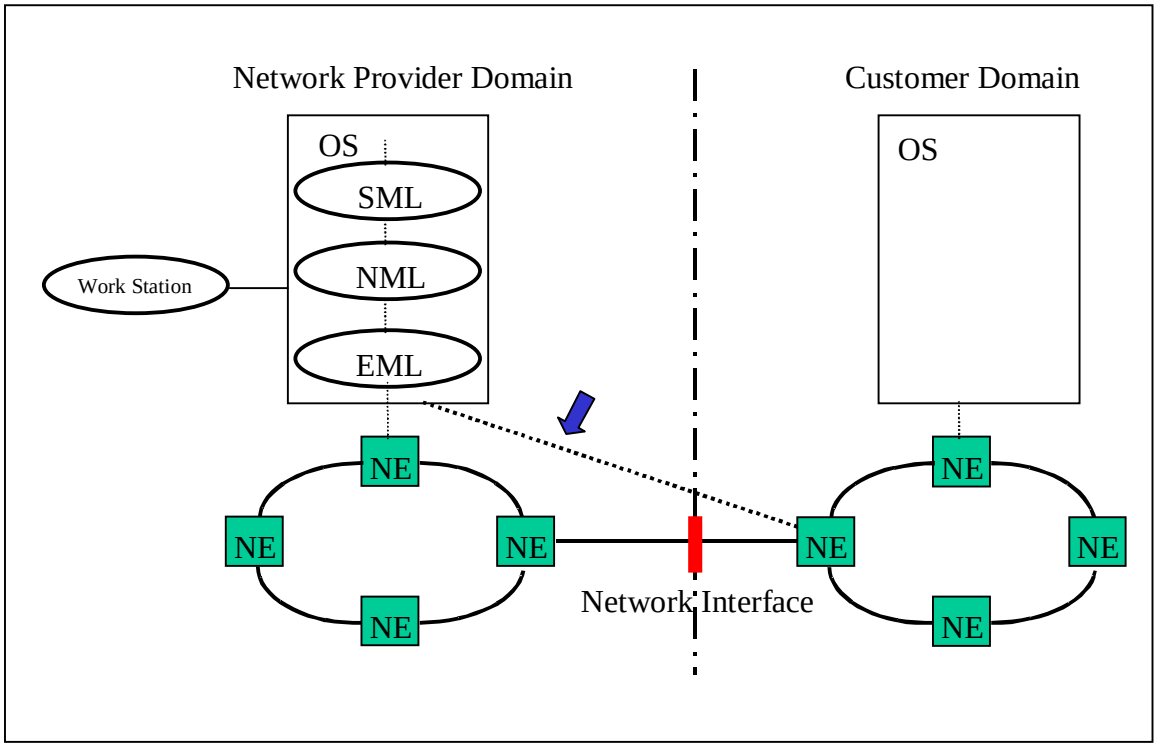

Figure 9 – Scenario 8: Customer NEs Managed by Network Provider OS Access

4 NSIF Security Requirements

For the types of interfaces that are within the scope of this document, and which are recommended for use in the Access Policy Scenarios section (Section 3), the following security functions are **required** to be supported:

- Entity identification - this is the basis for authentication and authorization
- Strong peer entity authentication using asymmetric encryption (Public-key technology) – both identities must be authenticated
- Authorization - this is usually accomplished with access control lists (ACLs) in the accessed entity or a security server. ACLs are the responsibility of the accessed entity and are not administered across the interface. Attribute certificates (ACs), when available can be included in the interface. Both ACLs and ACs **are not addressed** by this document.
- Message integrity using a cryptographic hash function – this allows for detection of any alteration to a message during communication

Message confidentiality (encryption) and non-repudiation functions are optional. These functions are not normally required for the types of interfaces that are the focus of this document. Security application functions such as security alarm reporting and security audit are recommended but **are not covered** in this document.

It is strongly recommended that Network Providers take measures to secure all OS, WS, CIT, NE and security server platforms and the data communications network (DCN) that connects them. This process is not covered in this document.

5 Public Key based Security

Public Key Infrastructure (PKI) is emerging as the lowest cost, scalable solution for TMN security. T1M1.5 is producing a set of PKI standards that are intended to promote interoperability among PKI components from different product suppliers and network providers, and to promote interoperability among different companies or administrations.

ANSI T1.268 - 2000, TMN PKI – Digital Certificates and Certificate Revocation List Profiles is the first in a series of ANSI standards devoted to PKI for a TMN.

The Accredited Standards Committee (ASC) X9 has issued a new standard, ANSI X9.79: 2000, *PKI Practices and Policy Framework*, that defines the components of a PKI and sets a framework of practices and policy requirements for its use. ASC X9 is the national standards-setting body for the financial services industry and is accredited by the American National Standards Institute (ANSI).

Several security protocols use public-key cryptography to provide services such as confidentiality, data integrity, data origin authentication, and non-repudiation. The purpose of a PKI is to provide trusted and

efficient key and certificate management, thus enabling the use of strong authentication, non-repudiation, and confidentiality.

5.1 High Level Overview of the TMN PKI

The TMN PKI consists of the following **components**:

A **Certification Authority** (**CA**) produces **public key certificates** for all the TMN entities that need to have secure communications, as well as for any external entities that need to communicate securely with TMN entities. A CA also issues certificates to CAs outside the TMN. The CA issues **Certificate Revocation Lists (CRLs**) as necessary. A CRL includes the serial numbers of certificates that have been revoked (for example, because the key has been compromised or because the subject is no longer with the company) and whose validity period has not yet expired. The CA typically employs a tamper-proof computer kept under the highest physical security. The term CA is also used to refer to an organization (rather than a device) that issues certificates as a service, usually for a fee.

The most common format of a certificate is as defined in ITU-T Recommendation X.509 version 3 (X.509v3). X.509v3 defines several mandatory fields. It further provides for the addition of any number of **extensions**. Each extension is marked critical or non-critical. If an entity processing a certificate encounters a non-critical extension it does not recognize, it ignores that extension. If an entity processing a certificate encounters a critical extension it does not recognize, it must reject the certificate. X.509v3 also allows extensions to CRLs and to individual CRL entries. Interoperability in a TMN or between TMNs requires, at a minimum, full agreement on all critical extensions (if any) in certificates used in TMN applications. ANSI standard T1.268 provides profiles for certificate extensions and CRLs.

A **Registration Authority (RA)** verifies the authenticity of every entity (NE, OS, WS, employee, customer, supplier, etc.) that should receive public key certificate from the TMN's CA. The RA typically consists of a small number of security administrators with access to the CA.

An RA typically publishes a **Certification Policy Statement (CPS)** that specifies under what conditions (e.g., identity check) it would issue a certificate.

PKI includes a **directory** for the storage and distribution of certificates and CRLs. ITU-T Recommendation X.500 provides the basis for the directory. ANSI standard T1.245 specifies a X.500 directory for the TMN. ANSI standard T1.252 provides the specifications for a secure TMN directory. T1.252 is based on the X.500 DAP (Directory Access Protocol). However, directories based on the IETF PKI profile of LDAPv3 (Lightweight DAP, a subset of DAP) may be more readily available than directories based on T1.252.

Each **TMN entity** would need to interact with the TMN PKI directory in order to retrieve and receive certificates of other entities as well as CRLs. It would need the capability of processing certificates and CRLs.

The TMN PKI components need to interact through standard **protocols**. The interactions among TMN PKI components are illustrated in Figure 10.

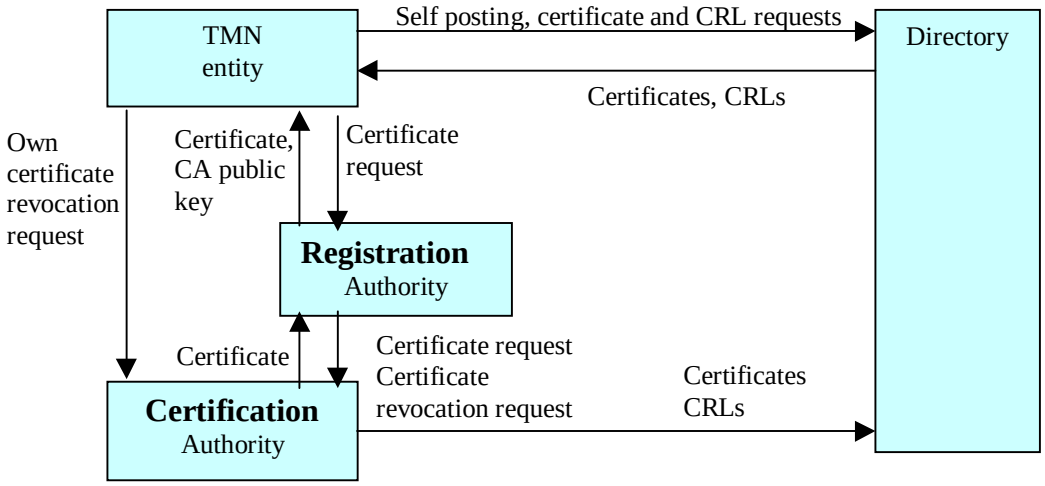

Figure 10: Interactions among TMN PKI components

5.2 Impact on Interfaces Addressed by This Document

For the Interfaces (e.g., NMS-EMS) addressed by this document, there are three separate (but related) security concerns. The first concern is the application protocol used across the interface (see Section 7). The second concern is the underlying communications protocol stack used across the interface, and whether or not this stack includes a security protocol (e.g., SSL3) that is capable of using public-key cryptography. The third concern (assuming that public-key cryptography will be used) is the management of keys and certificates. It is this third concern for which PKI provides a solution. The impact of PKI is that it requires the infrastructure components (CA, RA, Directory) to be in place, and it also requires that the TMN entities (e.g., NMS, EMS, etc.) have a mechanized way in which to communicate with the PKI components (particularly the Directory) for the purposes of key and certificate management.

6 Common Security Methods

Using consistent methods across all operations interfaces has the potential to reduce administration and security infrastructure costs, increase the likelihood of interoperability, and speed the deployment of security implementations. NSIF proposes that the Secure Socket Layer Protocol, Version 3.0 (SSL3) be used as a basis for common security methods for managing the network technologies that are of interest to NSIF. SSL, which was originated by Netscape, provides for security at the transport layer of the Transport Control Protocol/Internet Protocol (TCP/IP) protocol suite, and therefore is relatively transparent to applications. Optionally, the Transport Layer Security (TLS) Protocol, Version 1.0 may also be supported along with SSL3 (see RFC 2246).[1]

[1] The TLS protocol itself is based on the SSL 3.0 Protocol Specification as published by Netscape. The

SSL3 is widely used for securing web traffic, such as for Hypertext Transport Protocol (HTTP). But it can also be used for non-web communications, such as Common Object Request Broker Architecture (CORBA), and potentially could be used for any application protocol that is transported with TCP/IP. SSL3 rides between TCP/IP and the application protocol. It envelops the application messages and provides end-to-end transport security. SSL3 provides for three of the four requirements identified in Section 4: entity identification, strong peer entity authentication,and message integrity. SSL3 also provides confidentiality, which may be optional for network management functions performed within a single TMN. SSL3 does not provide for authorization functions.

It is a **Required Option** that any OS or NE providing a TCP/IP stack for operations messages also be capable of supporting SSL3. This would apply independently of which application layer protocol is used. This means that suppliers would be required to provide SSL3 support at the request of a network provider for any given NE, however, they otherwise would not be obligated to provide SSL3 on every NE. Likewise if network providers are not prepared to implement SSL3 on every TCP/IP operations interface, then a further differentiation can be made between *static* conformance to this requirement and *dynamic* conformance to this requirement as explained below:

- ***Static conformance***: The interface is capable of running SSL3, however, SSL3 does not necessarily have to be used on the interface.[2]
- ***Dynamic conformance***: The interface always runs SSL3.

SSL3 shall be used to secure the communications scenarios described in Section 3 of this document with the following guidelines:

- Strong peer entity authentication, based on public key encryption shall be provided for all associations (this precludes interoperability with SSL2)
- Session secret shall be encrypted with receiver's public key
- Message encryption is optional
- Secure Hash Algorithm (SHA)1 shall be used for message integrity
- Non-repudiation or message integrity can be provided, optionally, by higher layers
- Every participant (entity) is required to obtain a public key certificate from a CA selected by the network provider
- Entity public key size shall be at least 1024 bits
- Certification Authority's public key size shall be at least 2048 bits
- Certificates shall be X.509 version 3.

---

differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough that TLS 1.0 and SSL 3.0 do not interoperate (although TLS 1.0 does incorporate a mechanism by which a TLS implementation can back down to SSL 3.0).

[2] The motivation for this is to give the network provider the flexibility to run SSL3 as they see fit.

- The following cipher suites will be supported:
  - CipherSuite SSL_RSA_WITH_NULL_SHA
  - CipherSuite SSL_RSA_WITH_DES_CBC_SHA (if optional confidentiality is desired)
- Resumable sessions do not present any additional threat

T1M1.5/2000-154, *Security Services and Algorithms for TMN*, which is being drafted, should be referenced when completed for the most current security mechanisms and algorithms.

7 Management Protocols of Interest

Until recently, there were only two management protocols that were accepted as the direction for communications in the TMN environment: Common Management Information Service Element (CMISE) for interactive communications, and File Transfer, Access and Management (FTAM) for file transfer. But within the last year or two, more generic computing protocols have been assessed for telecommunications use such as CORBA and File Transfer Protocol (FTP). ANSI T1.271, *Framework for CORBA-Based Telecommunications Management Network Interfaces*, defines CORBA services and programming conventions that are suitable for the TMN environment. ANSI T1.270, *CORBA Generic Network and NE Level Information Model*, defines a generic CORBA model similar to that defined in ITU Recommendations X.721 and M.3100. Similar standards have been developed in ITU-T – Q.816, *CORBA-based TMN Services*, X.780, *TMN Guidelines for Defining CORBA Managed Objects*, and M.3120, *CORBA Generic Network and Network Element Level Information Model*. It is expected that the choice of protocols for the TMN environment will increase in number over time since Information Technologies tend to change quickly. To maximize opportunities for interoperability and integration, it is recommended that the number of protocols for TMN interface types be limited as much as possible. The current direction for EMS-NMS Q interfaces is CORBA, and may possibly be the direction for NE-EMS interfaces.

There are two protocols that are considered embedded base: TL1 and SNMP. These are primarily used as NE-EMS communications and will probably continue to be used for some time. SNMP in particular is still actively being enhanced.

There is also a trend toward browser-based craft interface devices, especially as Ethernet connections become more common in Central Offices. HTTP, which is used for browsers, can support various languages such as eXtensible Mark-up Language (XML) and Java™™.

In summary, the current application protocols of interest for performing network management functions are TL1, CORBA, SNMP, HTTP and FTP. Although some North American carriers are no longer proposing CMISE for new interfaces, it is included in this document because of security work done earlier in the SONET Interoperability Forum.

Figure 11 shows the area of focus of this document and the protocols that are most likely to be used at the interfaces. FTP, which is not shown in the figure, can be used at all of the interfaces.

™ Java is a Trade Mark of Sun Microsystems, Inc.

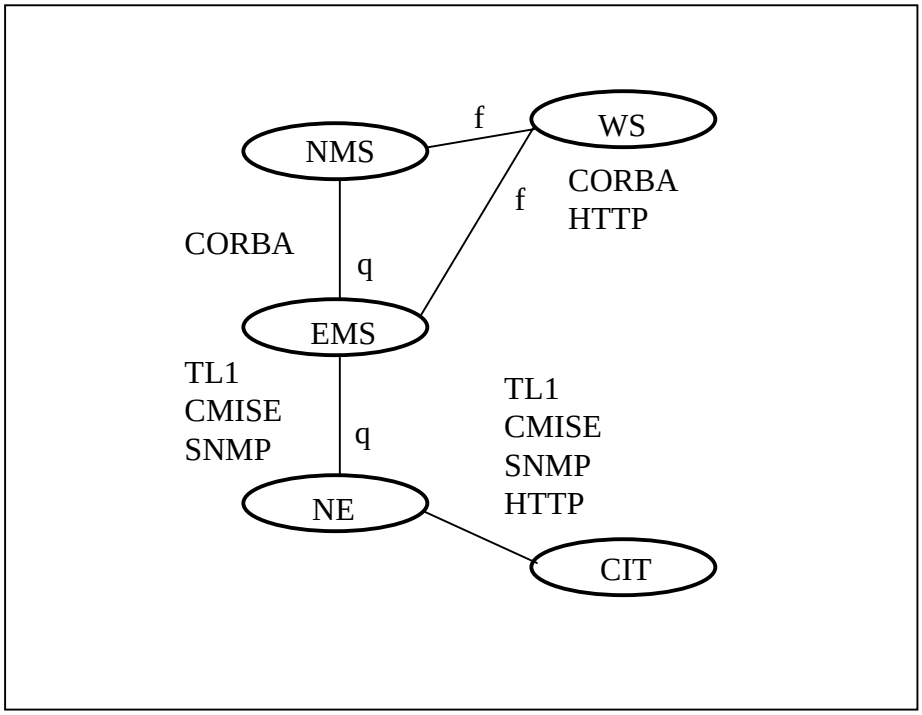

Figure 11 – Mapping of Protocols to Interfaces

8 Requirements by Management Protocol

The following sub-sections define the security requirements for the protocols of interest.

8.1 TL1

The TL1 management protocol is currently used by some NEs at either the WS/NE interface, the OS/NE interface, or both interfaces. The security requirements that apply when using TL1 at the WS/NE interface and/or at the OS/NE interface are provided below.

WS/NE Interface

For the WS/NE interface, NSIF requires that the security requirements stated in Section 6.1.6 of Telcordia GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, be followed. According to NSIF-037-2000, *Common Applications Requirements for SONET NE Security System*, network providers may need an even greater level of security than what is specified by GR-253-CORE. In such instances, network providers may choose to also deploy a centralized security server according to the requirements provided by NSIF-038-2000, *NSIF Requirements for a Centralized Security Server*.

OS/NE Interface

For the OS/NE interface, NSIF requires that the security requirements stated in Section 6.1.6 of Telcordia GR-253-CORE be followed. Although some network providers have expressed a desire for an even greater level of security than what is specified by GR-253-CORE, there is a general consensus among NSIF members that NSIF should not attempt to define additional security features for TL1-based OS/NE interfaces at this time. However, when TL1 is used via the TL1 over TCP/IP interface (e.g., see NSIF-033-1999), network providers do have the option of requesting that SSL3 as specified in Section 6, be provided by the NEs that support the TCP/IP interface.

8.2 CMISE

For Q interfaces that implement Common Management Information Protocol (CMIP) over an OSI stack, it is an objective that the interface support authentication of the association initiator, data origin authentication, message integrity and access control as specified in T1.261, *Security for TMN Management Transactions over the TMN Q3 Interface*.

For implementations that use CMIP over TCP/IP (with RFC1006), it is an **objective** that SSL3 be utilized to provide peer entity authentication and message integrity. Use of SSL3 is defined in TCIF-99-016, *Generic Guidelines for the Use of TCP/IP in Electronic Bonding.* It is also an objective that the interface support access control as specified in T1.261, *Security for TMN Management Transactions over the TMN Q3 Interface.*

When completed, T1M1.5/2000-154, (Draft) *Security Services and Algorithms for TMN*, should be referenced for the most current security mechanisms and algorithms.

Where the ACSE Authentication Functional Unit is not available to meet T1.261 requirements, or SSL3 with CMIP/TCP/IP is not available, a CMISE Q interface must at a minimum support simple application layer identification and authentication. Identification shall be based on the Application Entity Title (AE-Title) at association establishment time. Both the Manager and the Agent shall maintain a list of AE-Titles that are authorized to communicate with them. Two-way authentication of the communicating parties shall also be done at association set-up time. The authentication information (simple password) is carried in the accessControl field of the CMIPUserInfo structure. Prior to communication, the passwords for the Manager and Agent are stored securely in each others system and are later used for comparing with the CMIPUserInfo passwords.

8.3 CORBA

The Object Management Group (OMG) states in their CORBA *Security Services Specification*:

> "An ORB must meet the following requirements to claim conformance to the CORBA Security specification:
>
> - To claim conformance to the CORBA Security interfaces it must support the following feature packages:
>   - Security Functionality Level 1.

- To claim conformance to CORBA Secure Interoperability it must support the following feature packages:
    - Secure Interoperability using SECIOP.
    - Common Secure Interoperability (CSI) Level 1.
    - GSS Kerberos Protocol using MD5 Cryptographic profile."

"Conformance can be claimed for CORBA Security based on SSL by providing CSI level 0 functionality using SSL on IIOP using any of the cryptographic profiles defined in SSL. A conformant ORB must specify which of the cryptographic profiles are supported by it."[3]

T1M1.5 in T1.271, *Framework for CORBA-based TMN Interfaces*, has stated:

> The CORBA interface may optionally support either the "Secure IOP protocol," or "CORBA Security SSL Interoperability," as defined in the CORBA Security Specification.

To provide consistency in security methods, NSIF prefers the SSL3 solution. It is a **Required Option** that SSL3 be utilized to provide peer entity authentication and message integrity for CORBA interfaces.

8.4 SNMP

Currently, the IETF, which is the keeper of SNMP standards, is encouraging the use of SNMPv3 when secure SNMP communications is required. SNMPv3 has its own security mechanisms for authentication, access control and message integrity. This would extend the use of SNMP to configuration functions, whereas today, with SNMPv1 and SNMPv2, it is primarily used for monitoring.

SNMP runs over UDP/IP, and as such is not a candidate for use with SSL3. However, there is an Internet Draft defining its use with TCP/IP for cases where large packets are transferred. In time, if SNMP over TCP/IP becomes prevalent for telecommunications management, an SSL3 solution may be made available. Until this issue is resolved, it is a **requirement** that SNMPv3 be used with the User-based Security Model (USM) and View-based Access Control Model (VACM).

8.5 HTTP

Craft Interface devices, commonly referred to as CIT, are usually laptop PCs that are used for local access to an NE for installation, repair and other functions that cannot be done from a centralized operations center. There appears to be a trend for CIT applications to use a web browser platform and Hypertext Transfer Protocol (HTTP) for communications between the CIT and NE. HTTP 1.1 is specified in RFC2616.

SSL3 is commonly used with HTTP to provide secure web-based transactions. RFC2818 documents the

[3] Bold type has been added here for emphasis.

use of HTTP with TLS. Figure 12 shows the protocol stack for HTTP with SSL3 or TLS. When SSL3 is used, the Uniform Resource Locator (URL) shown in the browser's location field begins with "https".

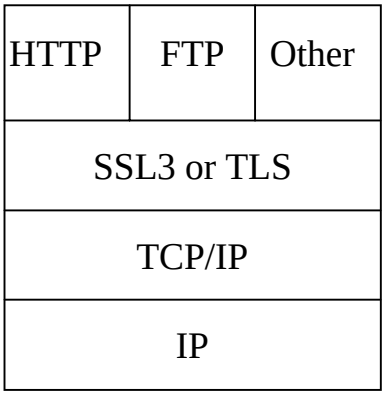

Figure 12 - HTTP/SSL Protocol Stack

When HTTP is used for Workstation access to OS, support of SSL3 is a **Required Option**.

It is an **Objective** to use SSL3 when HTTP is used for CIT access to an NE. The NE will need to access a PKI-based security server or directory server to periodically get an updated Certificate Revocation List (CRL) or to obtain a person's authorization information. However, it may be some time before a Public Key Infrastructure is available for NEs. Therefore in the interim, HTTP access is **Required** to be through a security server as described in NSIF-038-2000, *NSIF Requirements for a Centralized Security Server*. It is a **Required Option** that HTTP access to the secruity server use SSL3 security. When connectivity between the security server and the NE is not available, a UserID and password must be used to access the NE.

8.6 FTP

When using FTP for transferring files between OSs, WSs, NEs and CIT, it is a **Required Option** to use FTP with SSL3 when this feature is available. An IETF Internet Draft (draft-murray-auth-ftp-ssl-07.txt) describes how to provide TLS support for FTP in a similar way to that provided for HTTP. The document allows the FTP protocol to be used with either SSL3 or TLS. The actual protocol used will be decided during the TLS/SSL3 negotiation. The negotiated cipher suites must include support for peer authentication and message integrity (see Section 6 of this NSIF document).

The IETF draft named above requires some of the FTP extensions that are defined in RFC2228, *FTP Security Extensions*.

When FTP with SSL3 is not available refer to NSIF-033-1999, *Requirements for the TCP/IP Protocol Suite on the SONET Access DCN*, for an interim solution.

9 References

GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, Telcordia, Issue 3, September, 2000

SIF-010-1998, *Intercarrier Interface Recommendations*

NSIF-033-1999, *Requirements for the TCP/IP Protocol Suite on the SONET Access DCN*

NSIF-037-2000, *Common Applications Requirements for SONET NE Security System*

NSIF-038-2000, *NSIF Requirements for a Centralized Security Server*

NSIF-039-2000, *NSIF Reference Architectures*

ANSI T1.233-1999, *OAM&P – Security Framework for TMN Interfaces*

ANSI T1.245-1997, *Directory Service for TMN and SONET*

ANSI T1.252-1996, OAM&P – *Security for the Telecommunications Management Network (TMN) Directory*

ANSI T1.261-1997, OAM&P - *Security for TMN Management Transactions over the TMN Q3 Interface*

ANSI T1.268-2000, *TMN PKI – Digital Certificates and Certificate Revocation Lists Profiles*

ANSI T1.270-2000, *CORBA Generic Network and NE Level Information Model*

ANSI T1.271-2000, *Framework for CORBA-based Telecommunication Management Network Interfaces*

T1M1.5/2000-154R1, *Security Services and Algorithms for TMN*, DRAFT, November 2, 2000

ITU-T Rec. M.3010, *Principles for a Telecommunication Management Network*, 2000

ITU-T Rec. X.500, *Opens Systems Interconnection – The Directory: Overview of Concepts, Models and Services*, 1997

ITU-T Rec. X.509, *Opens Systems Interconnection – The Directory: Authentication Framework*, 1997

ITU-T Rec. X.800, *Security Architecture for Open Systems Interconnection for CCITT Applications*, March 1991

ITU-T Rec. X.810, *Open Systems Interconnection – Security Frameworks for Open Systems: Overview*, November 1995

ITU-T Rec. Q.816, *CORBA-based TMN Services*, 2001

ITU-T Rec. X.780, *TMN Guidelines for Defining CORBA Managed Objects*, 2001

ITU-T Rec. M.3120, *CORBA Generic Network and Network Element Level Information Model*, 2001

IETF RFC2246, *The TLS Protocol Version 1.0*, January 1999

IETF RFC2228, *FTP Security Extensions*, October 1997

IERF RFC2251, *Lightweight Directory Access Protocol (v3)*, December 1997

IETF RFC2401, *Security Architecture for the Internet Protocol*, November 1998

IETF RFC2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*, April 1999

IETF RFC2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP3)*, April 1999

IETF RFC2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), April 1999

IETF RFC2616, *Hypertext Transfer Protocol - HTTP/1.1*, June 1999

IETF RFC2818, *HTTP over TLS*, May 2000

IETF Internet Draft, *Internet X.509 Public Key Infrastructure* (draft-ietf-pkix-roadmap-06.txt), November 2000

IETF Internet Draft, *Securing FTP with TLS* (draft-murray-auth-ftp-ssl-07.txt), April 2001

IETF Internet Draft, *SNMP over TCP Transport Mapping* (draft-irtf-nmrg-snmp-tcp-06.txt), March 2001

OMG Document formal/2000-06-25, *Security Services Specification*, Version 1.5, May, 2000

10 Acronyms

AC – Attribute Certificate

ACL – Access Control List

ACSE – Association Control Service Element

AE-title – Application Entity title

ASC – Accredited Standards Committee

CA – Certification Authority

CBC – Cipher Block Chaining

CIT – Craft Interface Terminal

CITF – Craft Interface Terminal Function

CLEC – Competitive Local Exchange Carrier

CMIP – Common Management Information Protocol

CMISE – Common Management Information Service Element

CNM – Customer Network Management

CORBA – Common Object Request Broker Architecture

CPS – Certification Policy Statement

CRL – Certificate Revocation List

CSI – Common Secure Interoperability

DAP – Directory Access Protocol

DCC – Data Communications Channel

DCN – Data Communications Network

DES – Data Encryption Standard

DWDM – Dense Wavelength Division Multiplexing

EML – Element Management Layer

EMS – Element Management System

FTAM – File Transfer, Access and Management

FTP – File Transfer Protocol

HTTP – Hypertext Transport Protocol

IETF – Internet Engineering Task Force

IIOP – Internet Inter-ORB Protocol

IP – Internet Protocol

IPSec – Internet Protocol Security

ISP – Internet Service Provider

LDAP – Lightweight Directory Access Protocol

MD5 – Message Digest 5

NE – Network Element

NEF – Network Element Function

NI – Network Interface

NML – Network Management Layer

NMS – Network Management System

OMG – Object Management Group

ORB – Object Request Broker

OS – Operations System

OSF – Operations System Function

OSC – Optical Supervisory Channel

OSI – Open Systems Interconnection

PKC – Public Key Certificate

PKI – Public Key Infrastructure

RA – Registration Authority

RFC – Request for Comments

RSA – Rivest Shamir Adelman

SECIOP – Secure Inter-ORB Protocol

SHA1 - Secure Hash Algorithm 1

SIF – SONET Interoperability Forum

SNMP – Simple Network Management Protocol

SML – Service Management Layer

SMS – Service Management System

SONET – Synchronous Optical NETwork

SSL – Secure Socket Layer

TCP – Transport Control Protocol

TL1 – Transaction Language 1

TLS – Transport Layer Security

TMN – Telecommunications Management Network

WS – Workstation

WSF – Workstation Function

XML – eXtensible Markup Language

11 Glossary

Definitions from existing standards are used where applicable. The source standard or NSIF document is noted in parenthesis.

Access Control - the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (X.800-1991)

Access Control List - a list of entities, together with their access rights, which are authorized to have access to a resource. (X.800-1991)

Accountability - the property that ensures that the actions of an entity may be traced uniquely to the entity. (X.800-1991)

Attribute Certificate (AC) – a set of attributes of a user together with some other information, rendered unforgeable by the digital signature created using the private key of the certification authority which issued it. (X.509-1997)

Authentication - the process of verifying the claimed identity of the session requester. For example, a password check, or smart card validation can serve as the process for this verification. (NSIF-038-2000)

Authorization - the granting of rights, which includes the granting of access based on access rights. (X.800-1991)

Certification Authority (CA) - an authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them. (IETF PKIX Roadmap)

Certification Policy - a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range. (X.509-1997)

Certificate Revocation List (CRL) - a time stamped list identifying revoked Public Key Certificates that is signed by a Certification Authority and made freely available in a public repository. (IETF PKIX Roadmap)

Confidentiality - the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (X.800-1991)

Cryptography - the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (X.800-1991)

Data Integrity - the property that data has not been altered or destroyed in an unauthorized manner. (X.800-1991)

Data Origin Authentication - the identity of the originator of a message is authenticated, without necessarily insuring the integrity of the message. (TI.261-1998)

Decryption - the reversal of a corresponding reversible encipherment. (X.800-1991)

Digital Signature - data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. (X.800-1991)

Directory – when used for security, a repository for PKI information.

Encryption - the cryptographic transformation of data (see cryptography) to produce ciphertext. (X.800-1991)

Hash Function - a mathematical function which maps values from a large set of values into a smaller range of values. (X.810-1995)

Identification - the process of recognizing a session requestor's unambiguous and auditable identity, such as a user-ID. (NSIF-038-2000)

Message Integrity – a process that allows for detection of any alterations of messages in a communication

Non-repudiation - protection against any attempt by the sender or recipient to falsely deny sending or receiving the data or its content. (T1.233-1993)

Peer Entity Authentication - the identity of each party in an association is authenticated to the other party. (T1.261-1998)

Private Key - (in a public key cryptosystem) that key of a user's key pair which is known only by that user. (X.509-1997)

Privilege Management Infrastructure (PMI) - the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Attribute Certificates. (IETF PKIX Roadmap)

Public Key - (in a public key cryptosystem) that key of a user's key pair which is publicly known. (X.509-1997)

Public Key Certificate - the public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. (X.509-1997)

Public Key Infrastructure (PKI) - the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography. (IETF PKIX Roadmap)

Registration Authority - an optional entity given responsibility for performing some of the administrative tasks necessary in the registration of subjects, such as: confirming the subject's identity; validating that the subject is entitled to have the values requested in a PKC; and verifying that the subject has possession of the private key associated with the public key requested for a PKC. (IETF PKIX Roadmap)

Security Administration - security administration consists of proper activation, maintenance, and usage of the security features of a system, conducted by an appropriate administrator. It includes, among other functions, overriding vendor-supplied defaults, ensuring appropriate backup procedures, "managing" the

security database (i.e., keeping up to date the data that represents security parameters), and generating security audits when needed. (NSIF-038-2000)

Security Policy - the set of rules laid down by the security authority governing the use and provision of security services and facilities. (X.509-1997)

Security Audit- an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. (X.800-1991)

Security Audit Trail - data collected and potentially used to facilitate a security audit. (X.800-1997)

Simple Authentication - authentication by means of simple password arrangements. (X.509-1997)

Strong Authentication - authentication by means of cryptographically derived credentials. (X.509-1997)