

NTCIP 1105 v01.02

National Transportation Communications for ITS Protocol CORBA Security Service Specification

April 20, 2001; based on v01.01 of August 24, 2000

This is a draft document, which is distributed for review and comment purposes only. You may reproduce and distribute this document within your organization, but only for the purposes of and only to the extent necessary to facilitate review and comment to the **NTCIP Coordinator**. Please ensure that all copies reproduced or distributed bear this legend. This document contains preliminary information which is subject to change.

Published by

American Association of State Highway and Transportation Officials (AASHTO)

444 North Capitol Street, N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)

1099 14th Street, N.W., Suite 300 West
Washington, D.C. 20005-3438

National Electrical Manufacturers Association (NEMA)

1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209-3801

© Copyright 2001 AASHTO / ITE / NEMA. All rights reserved.

ACKNOWLEDGEMENTS

This publication was prepared by the NTCIP Center-to-Center Working Group, a subdivision of the Joint Committee on the NTCIP. The Joint Committee is organized under a Memorandum of Understanding among the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA). The NTCIP development effort is guided by the Joint Committee on the NTCIP, which consists of six representatives from each of the above organizations.

At the time that this document was prepared, the following individuals were active members of the NTCIP Center-to-Center Working Group:

- Ken Vaughn
- Warren Tighe
- Greg Mosley
- Walt Townsend
- Allan Foodym
- Bob Rausch
- Ray Starr
- Jeff Mayo
- Steve Dellenback
- Jeff Brummond
- Blake Christie
- Scott Melby
- Paul Olson

In addition to the many volunteer efforts, recognition is also given to those organizations who supported the efforts of the working groups by providing comments and funding for the standard, including:

- ADF Consulting
- Federal Highway Administration
- Gardner Systems
- Iteris
- Minnesota Department of Transportation
- MitreTek Systems
- National Engineering Technologies
- PB Farradyne
- Southwest Research Institute
- Texas Department of Transportation
- TransCore
- Washington State Department of Transportation

FOREWORD

This document uses only metric units.

This publication defines the CORBA Security Service Specification for use in center-to-center communications in the transportation domain. There are no annexes to this document.

This document is an NTCIP Base Standard. Base Standards provide formal definitions of protocols or services upon which higher level applications are dependent for use within NTCIP systems.

For more information about NTCIP standards, visit the NTCIP Web Site at <http://www.ntcip.org>. For a hardcopy summary of NTCIP information, contact the NTCIP Coordinator at the address below.

In preparation of this NTCIP document, input of users and other interested parties was sought and evaluated. Inquires, comments, and proposed or recommended revisions should be submitted to:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

INTRODUCTION

This publication provides definitions of the CORBA Security Service Specification for use in center-to-center communications in the transportation domain.

This standard defines requirements that are applicable to NTCIP environments that use CORBA.

The following keywords apply to this document: AASHTO, ITE, NEMA, NTCIP, CORBA.

The effort to develop NTCIP began in 1992 with the 3-TS Transportation Management Systems and Associated Control Devices Section of NEMA. Their original desire was to address a user need for extending the TS 2 Standard for traffic control hardware to include standardized systems communication. Under the guidance of the Federal Highway Administration's (FHWA) NTCIP Steering Group, the NEMA effort was expanded to include the development of communications standards for all transportation field devices that could be used in an Intelligent Transportation Systems (ITS) network and for center-to-center communications.

In September 1996, a formal agreement was reached among NEMA, ITE, and AASHTO to jointly develop, approve, and maintain NTCIP Standards. The Center-to-Center Working Group commenced work in 1996.

CONTENTS

BACKGROUND	VI
SECTION 1 GENERAL	1-1
1.1 Scope.....	1-1
1.2 Protocol – Layer Relationship.....	1-1
1.3 References	1-1
1.3.1 Normative References.	1-2
1.3.2 Informative References.....	1-3
1.4 Definitions, Acronyms, and Terms	1-3
SECTION 2 REQUIREMENTS AND CONFORMANCE	2-1
2.1 General Requirements	2-1
2.2 Functional Requirements.....	2-1
2.2.1 Administrator Actor	2-2
2.2.2 User Actor	2-2
2.2.3 Filter User Access Use Case.....	2-2
2.2.4 Encrypt Communication Use Case.....	2-3
2.2.5 Report User Information.....	2-3
2.2.6 Store User Password Use Case	2-3
2.2.7 Input User Information Use Case	2-3
2.2.8 Store Security Information Use Case	2-3
2.2.9 Assign User Priority Use Case	2-3
2.2.10 Assign User Privilege Use Case.....	2-3
2.2.11 Authenticate User Use Case	2-3
2.3 Interface definitions	2-4
2.3.1 Security Access Interface	2-4
2.3.2 Object Access	2-8
2.3.3 Secure Communications.....	2-8
2.4 Operation.....	2-10
2.4.1 Login Sequence	2-10
2.5 IDL	2-11

BACKGROUND

Center-to-Center (C2C) communications, like any industry wide-area network, typically address secure communications within a security policy. This policy defines the rules by which all users of the network must abide. The depth of this policy depends on the network scope as well as network risk assessment. Analysis of the risks and how much exposure is tolerable will effect costs of the communication hardware and software. This specification considers the overall effects of a security policy but does not establish the policy itself; rather, the mechanism that underlies a policy. This C2C security mechanism considers the following three security issues:

- Risk Assessment
- Vulnerability
- Security Guidelines

Risk assessment is the process of finding out what data is transmitted and how important it is. In addition to the importance of the data is the amount of damage will incur if it is lost or compromised. Traffic information is not usually considered high risk data, since it usually deals with public telemetry data from field devices and not sensitive information. Compromise of this data can disrupt but will not severely impact traffic operations and is easily recovered. On the other hand, compromise of field device control, such as changeable signs, has larger security risks because of safety and legal considerations.

Looking around the network is the first step in assessing vulnerability. Most network intrusions are from the inside, not the outside. Hackers and crackers make up just a small portion of the network compromises that are recorded annually. The vulnerability of C2C is dependent on the vulnerability of each agency connected. It is recommended therefore that each agency configure and maintain a firewall to the C2C network. It is also recommended that each agency maintain their workstations and servers in a secure area, which is locked and has restricted access. If someone can gain physical access to the servers, the servers can be compromised and also the network.

Agencies that are connected to the Internet should protect themselves and the C2C network through the proper use of firewalls. Also restricted use of dial-in modems is essential. If someone is using a modem to connect to the Internet while also connected to an agency's network, then there is a significant security hole. The best firewall is of no avail if people are bypassing them by using a modem to connect to their personal Internet accounts.

The C2C Security Service provides password protection to traffic data and device control at each center. Remote users must provide a user name and password in order to connect to the information/control interfaces. Associated with the user is his privileges and priority to access data and control devices. Passwords can be an open door to the network when poorly administered; often they are easily cracked or worse, just left laying around. A good password policy should be in place and enforced.

Section 1 GENERAL

1.1 SCOPE

This specification is written for CORBA based systems as defined by the CORBA Center-to-Center profiles. The requirements herein are tailored to the capabilities inherent in a CORBA network and will not necessarily work with other Center-to-Center protocols. The overarching objective is to give each transportation center full control over its data resources. Therefore, this specification defines a Security Service that will authenticate external users and allow them certain privileges and priorities to access data and control devices. While there are many solutions to security, this specification chooses a single approach that can be implemented using most off-the-shelf CORBA products. This specification does not impose security requirements on all transportation centers, but rather on those centers that choose secure CORBA communications to protect their resources.

1.2 PROTOCOL – LAYER RELATIONSHIP

This specification describes the required interfaces of the Security Service. Within the scheme of the ISO OSI 7-Layer Reference Model, the Security Service is within the Application and Session Layer. As a high-level service, it requires other application-layer services, such as a CORBA ORB and its associated protocols, to be in place. Table 1 shows the place of Security Service.

Table 1 - Security Service - Base Standard Relationship

NTCIP Profiles	ISO Layers	Base Standard
APPLICATION PROFILE	APPLICATION LAYER	Security Service (this standard)
	PRESENTATION LAYER	(not addressed by this standard)
	SESSION LAYER	Security Service (this standard)

1.3 REFERENCES

For approved revisions, contact:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 N.17th Street, Suite 1847
Rosslyn, Virginia 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

For draft revisions of this document, which are under discussion by the relevant NTCIP Working Group, and recommended revisions of the NTCIP Joint Committee, visit the World Wide Web at <http://www.ntcip.org>.

The following standards (normative references) contain provisions, which through reference in this text, constitute provisions of this Standard. Other documents and standards (other references) are referenced in these documents, which might provide a complete understanding of the structure and use of profiles. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.