Standard Security Label for the Government Open Systems Interconnection Profile (DRAFT)

Federal Information Processing Standards Publication DRAFT 1992 July 15
DRAFT

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

CATEGORY: ADP OPERATIONS

SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Barbara Hackman Franklin, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, John W. Lyons, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official publication relating to standards and guidelines adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235. These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal Government. The NIST, through the Computer Systems Laboratory, provides leadership, technical guidance, and coordination of Government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

James H. Burrows, Director
Computer Systems Laboratory

Abstract

This Standard specifies a security label for the U.S. Government Open Systems Interconnection Profile (GOSIP). GOSIP security labels indicate to protocol entities how to handle unclassified but sensitive data communicated between open systems. Information carried by the label described here can be used to control access, specify protective measures, and indicate other handling restrictions required by a communications security policy. The specification for this security label is given in Abstract Syntax Notation 1 (ASN.1) form, an implementation independent notation. A label encoding for use at the Network and Transport Layers is given in an Appendix.

Key words: ADP security, U.S. Government Open Systems

Interconnection Profile (GOSIP) security, network

security, security labels, trusted Open Systems

Interconnection (OSI)

Federal Information

Processing Standard Publication XXX DRAFT 1992 July 15 DRAFT ANNOUNCING A Standard Security Label for the Government Open Systems Interconnection Profile Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

Name of Standard: Standard Security Label for the Government Open Systems Interconnection Profile.

Category of Standard: ADP Operations, Computer Security.

Explanation: This Standard gives an implementation independent specification of a security label for the U.S. Government Open Systems Interconnection Profile (GOSIP). Security labels indicate sensitivity and the possible damage which may occur due to accidental or intentional disclosure, modification, or destruction of data. Labels are used to make access control decisions, to specify protective measures, and to indicate handling restrictions required by a communications security policy. The Standard Security Label is intended for use on U. S. Government OSI networks that exchange unclassified but sensitive data.

The label presented here defines security tags that may be combined into tag sets to carry security-related information. Five basic security tag types allow the representation of bit maps, attribute enumerations, attribute range selections, security level indication, and of generic information in a free form field.

A Computer Security Objects Register (CSOR), established by NIST, will provide the semantics for labels represented using this standard. Documents referencing this labeling standard shall either point to a CSOR and its procedures for registration of labels, or provide all the pertinent information regarding the label(s) to be supported.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Computer Systems Laboratory, National Institute of Standards and Technology.

Cross Index:

Federal Information Resources Management Regulations, subpart 201-20.303, Standards, and subpart 201-39.1002, Federal Standards.

"Procedures for Registration of Computer Security Objects", NIST 1992.

"U.S. Government Open Systems Interconnection Profile" (GOSIP), FIPS PUB 146-1, April 1991.

Scope: This standard specifies, in abstract notation, a security label for GOSIP-compliant implementations. Following this implementation independent specification, security labels may be encoded for use within various Open Systems Interconnection (OSI)

protocols. The Abstract Syntax Notation 1 (ASN.1) label description provided here shall be used for security labels in

Application Layer protocols. A normative Appendix to this standard provides the label encoding for the Network and Transport Layers. Other encodings of this Standard Label may be produced for use at the remaining layers if necessary. The specification given here is limited to the syntactic aspect of the label. The semantics of security labels, as defined for different security domains, are given by a Computer Security Objects Register.

Applicability: The specified Standard Security Label (SSL) applies to OSI communications systems handling U.S. government unclassified but sensitive data. This security label type shall be used by OSI systems required to label data as indicated in the security chapter of GOSIP.

The SSL shall be used by OSI protocols to control access, specify protective measures, and indicate handling restrictions required by a network security policy as registered in a Computer Security Objects Register.

Complying implementations shall be capable of transmitting, receiving, and handling security labels based on the high level specification in this document.

- Specifications: Federal Information Processing Standard (FIPS xxx)
- Standard Security Label for the Government Open Systems
- Interconnection Profile (affixed).

Implementation Schedule: This standard becomes effective six months after publication of a notice in the Federal Register of its approval by the Secretary of Commerce.

Waiver Procedure: Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:

- a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or
- b. Compliance with a standard would cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Technology Building, Room B-154, Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any accompanying documents, with such deletions as the agency is authorized and decides to make under 5 United States Code Section 552(b), shall be part of the procurement documentation and retained by the agency.

Special Information: References to this standard will appear in the security chapter of the U.S Government Open Systems Interconnection Profile (GOSIP) in a planned version 3 and future versions. Modifications to the planned version 3 will maintain backwards compatibility with the labeling options defined for the Connectionless Network Protocol (CLNP) in the first two versions. NIST plans that security protocols added to GOSIP in the future that require security labels will only use the Standard Security Label described in this document.

Where to Obtain Copies: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication XX (FIPS PUB XX), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

- Federal Information
- Processing Standard Publication xxx

DRAFT 1992 July 15 DRAFT

Specifications for a Standard Security Label for the Government Open Systems Interconnection Profile

1. INTRODUCTION

U.S. Government agencies are required to protect data essential to their operations. This requirement covers data stored, processed, and transmitted by computer and communications systems. This standard defines, in abstract notation, a security label type for use in the U.S. Government Open Systems Interconnection (OSI) Profile (GOSIP, FIPS PUB 146-1) [10]. GOSIP is a mandatory set of specifications for procurement of OSI communications systems.

The security label specified here may be used to indicate data sensitivity and possible damage due to accidental or intentional disclosure, modification, or destruction. Labels following this specification can be used to make access control decisions, specify protective measures, and indicate handling restrictions required by the applicable security policy.

The Abstract Syntax Notation 1 (ASN.1) [4] is used to define the Standard Security Label (SSL). ASN.1 provides an implementation independent means of expressing complex Application Layer protocol elements. ASN.1 specifications are typically encoded using the Basic Encoding Rules (BER) [5], although other encodings may be used.

Our security labeling approach takes advantage of this flexibility to specify a common label type for use throughout the OSI stack. The ASN.1 specification of the SSL can be encoded to conform to specific layer protocols. This standard provides the encoding for security labels at OSI layers 3 and 4 in a normative appendix. Documents calling for encodings of the SSL for use at layers other than 3 and 4, shall provide such encoding or a reference to the document providing the encoding.

The SSL provides a set of tools that can be combined to support different security policies. Instances of this type of labels are registered in a Computer Security Objects Register (CSOR) where the rules for their interpretation are given. The CSOR associates a unique object identifier to each label definition provided thus enabling implementations to identify the labels and process them accordingly. Documents referencing this FIPS shall indicate the source and all information necessary for the use and implementation of the labels to be supported. This includes the identity of the CSOR, identifiers, and definitions for all labeling objects supported.

2. REFERENCES

[1] European Computer Manufacturers Association, "Security in Open

Systems - Data Elements and Service Definitions", ECMA

Standard 138, December 1989.

[2] International Standards Organization (ISO), "Information

processing systems - Open Systems Interconnection - Basic Model", ISO 7498, 1988.

[3] International Standards Organization (ISO), "Information processing systems - Open Systems Interconnection - Security Addendum", ISO 7498/2, 1988.

[4] International Standards Organization (ISO), "Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)", ISO/IEC 8824 (DIS), 1990.

[5] International Standards Organization (ISO), "Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)", ISO/IEC 8825 (DIS), 1990.

[6] Internet CIPSO Working Group, "Commercial IP Security Option", Proposed Request for Comments (RFC), February 7, 1991.

[7] Nazario Noel, "Security Labeling in Unclassified Networks", Proceedings of the 13th National Computer Security Conference, Volume 1, pp. 44-48, October 1990.

[8] Nazario Noel, "Security Labels for Open Systems - An Invitational Workshop", NISTIR 4362, June 1990.

[9] Nazario Noel, "Standard Security Label for GOSIP - An Invitational Workshop", NISTIR 4614, June 1991.

[10] "U.S. Government Open Systems Interconnection Profile"

(GOSIP),
FIPS PUB 146-1, April 1991.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms

CSOR - Acronym for Computer Security Objects Register.

GOSIP - Acronym for (U.S.) Government Open Systems

Interconnection Profile. GOSIP, or Federal Information

Processing Standard (FIPS) 146-1, is a procurement

profile for open systems computer network products. [10]

OSI - Acronym for Open System Interconnection.

PDU - Acronym for Protocol Data Unit.

TSN - Acronym for Tag Set Name.

3.2 Definitions

computer security object - (CSO). A resource, tool, or
mechanism used to maintain a condition of security in a

computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.

Computer Security Objects Register - (CSOR). A collection of CSO names and definitions kept by a registration authority.

domain - See security domain.
entity - An active element in an open system. [2]
open system - A set of one or more computers, the associated
software, peripherals, terminals, human operators, physical
processes, information transfer means, etc., that forms an
autonomous whole capable of processing and/or transferring
information that complies with the requirements of OSI
standards. [2]

Open Systems Interconnection - This term qualifies standards for the exchange of information among systems that are "open"to one another for this purpose by

virtue of their mutual use of applicable standards. The Basic reference model for OSI is given in [2].

protocol data unit - A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.[2]
policy - See security policy
protocol entity - Entity that follows a set of rules and formats (semantic and syntactic) that determine the communication behavior of other entities. [2]

Registered Field - An instance of an entry to the Computer Security Objects Register (CSOR) as carried in the label. Contains a Tag Set Name and a set of tags.

registration authority - Organization responsible for the maintenance of a branch of the ISO naming hierarchy.

security attribute - A security-related quality of a security object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes.

security domain - A collection of entities to which applies a single security policy executed by a single security administrator. [1]
security label - A marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. [3]
security policy - A set of criteria for the provision of security services that provide adequate protection for systems and data transfers. [3] A set of rules that define and constrain the activities of a data processing facility in order to maintain a condition of security. [1]

security tag - Information unit containing a representation of certain security-related information (e.g., a category bit map).

security threat - Circumstance with the potential to cause loss or harm to a computer system or the information it handles.

Tag Set Name - Unique object identifier associated with a set of security tags.

4. SECURITY LABEL SPECIFICATION

The Abstract Syntax Notation 1 (ASN.1) [4] definition of the Standard Security Label (SSL) is given in Figure 4.1 below. This definition shall be encoded as appropriate to the layer where it will be used. At the Network and Transport Layers, the encoding given in the appendix shall be used.

ZDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD DDDDDDDDDDDDDDDDDDDDDDDDDD

D

3 ASN.1 Definition for Standard Security Label

3

3
3
3 Standard Security Label ::= IMPLICIT SET OF RegisteredField

3

3
3
3 RegisteredField ::= IMPLICIT SEQUENCE {

3

3

3 tagsetname TagSetName,

3

3

3 securityTags SEQUENCE OF SecurityTag }

3

3

3

3 TagSetName ::= OBJECT IDENTIFIER

3

3

3

3 SecurityTag ::= CHOICE {

3

3
3 -- Type 1

3

3 bitMap [1] IMPLICIT BIT STRING,

3

3

3 -- Type 2

3

3 enumeratedAttributes [2] IMPLICIT SET OF SecurityAttribute,

3

3

3 -- Type 3

3

3 rangeset [3] IMPLICIT SET OF SecurityAttributeRange,

3

3

3 -- Type 4

3

3 securityLevel [4] IMPLICIT SecurityAttribute,

3

3

3 -- Type 5

3

3 freeFormField [5] IMPLICIT ANY DEFINED BY TagSetName }

3

3

3

3 SecurityAttributeRange ::= IMPLICIT SEQUENCE {

3

3

3 upperBound SecurityAttribute,

3

3

3 lowerbound SecurityAttribute }

3

3

3

3 SecurityAttribute ::= IMPLICIT INTEGER (0..65535)

3

3

@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDDD

D

Figure 4.1

5. EXPLANATION AND USAGE

According to the above abstract definition for the (SSL), a security label is defined as a collection of Registered Fields. These Registered Fields contain security information required by an organization's security policy. This information is used to maintain the security condition of a resource (e.g., communications system, data file, application process).

3DDDDDDD Standard Security Label DDDDDD3

ZDDDDDDDDDDDDBDDDD DDDBDDDDDDDDDDDD?

3 Registered 3 3 Registered 3

3 Field 1 3 ___ 3 Field N 3

@DDDDDDDDDDDDADD DDDDDDADDDDDDDDDDDDY

Figure 5.1

5.1 Registered Fields

Registered Fields are an instance of a security label registered in a Computer Security Objects Register (CSOR). A Registered Field has two parts, a security tag set name (TSN), and a security tag set. The TSN is an unique name associated with the semantics for interpreting the security tags carried in the field. The security tags carry the actual security information. A Registered Field is depicted in Figure 5.2. Every SSL must carry, at least, one Registered Field. The use of multiple Registered Fields in a single label provide for protection under multiple security

policies. This is useful for maintaining an appropriate degree of protection when information is shared across security domain boundaries. Implementations shall be able to scan the whole label even if a Registered Field is not recognized. Failure to recognize a Registered Field may constitute a security relevant event. The system security policy is responsible for identifying those events whose occurrence is relevant and indicating the action to follow.

3DDDDDDDDDDD Registered Field DDDDDDDDDD3

ZDDDDDDDDD?ZDDDDDDDDDDBD DDDDDBDDDDDDDDDD?

3 Tag Set 33 Security 3 3 Security 3

3 Name 33 Tag 3 ___ 3 Tag 3

@DDDDDDDDDY@DDDDDDDDDDADDDD DADDDDDDDDDDY

Figure 5.2

5.2 Security Tag Set Name

Security tag set names (TSNs) uniquely identify the labeling scheme supported by the data in the set of security tags that follow. A Computer Security Objects Register (CSOR) maintains the semantics necessary for interpretation of label information. The Register assigns unique TSNs based on a hierarchy of registration authorities. These unique names are described in terms of Object Identifiers as defined for the Abstract Syntax Notation 1 (ASN.1) [4]. Documents referencing this labeling standard shall either point to a CSOR and its procedures for registration of labels, or indicate the TSN and definition of the label(s) to be supported.

5.3 Security Tag Set

The set of security tags in each Registered Field carry the security information. Five tag types are defined in this standard. These tag types are, (1) Bit Map, (2) Enumerated, (3) Range, (4) Security Level, and (5) Free Form. Any combination of tag types may be used to represent the security information required by the local security policy for protection of the data being exchanged. This standard relies on the services of a Computer Security Objects Register to maintain the tag-specific information necessary for the correct implementation of labels. Upon registration, the value and significance of the following items shall be provided:

_number of tags,

_number of tags of each type,
_length of the set,
_length of each tag,
_ordering of tags,
_security relevant conditions,

The above list may be augmented by the Registration Authority for the CSOR.

5.3.1 Security Tag Type 1

Tag type 1 is the Bit Map Tag Type. Tags of this type are used to convey security parameters, such as compartments and protection categories, that may be selected from a set by setting a one-bit flag to a predefined value (logic 0 or 1). The use of either 0s or 1s to mark the set condition of the individual bits allows the implementation of permissive (e.g., release markings) and restrictive (e.g., categories) markings using the same mechanism to test both conditions.

5.3.2 Security Tag Type 2

Tag type 2 is the Enumerated Tag Type. Tags of this type are used when only a few security attributes out of a large set need to be singled out when labeling a given protocol data unit (PDU). This is done by assigning a fixed-size non-

negative binary number to each security attribute and enumerating those attributes that apply (set inclusion), or do not apply (set exclusion). This enumeration shall start with the lowest numbered attribute following an ascending order.

The entry registered in the CSOR will indicate whether attributes enumerated in a type 2 tag will be interpreted as included or excluded from the applicable set.

5.3.3 Security Tag Type 3

Tag Type 3 is the Range Tag Type. Tags of this type are used when all the security attributes between certain lower and upper bound need to be singled out when labeling a PDU. This is done by indicating the higher-numbered and lower-numbered attributes as bounds for the range. The entry registered in the CSOR will indicate whether attributes in a range will be interpreted as included or excluded from the applicable set.

A single tag may indicate multiple security attribute ranges.

These ranges shall be listed in descending numerical order and shall not overlap. Each upper or lower bound attribute is indicated by a fixed size number.

5.3.4 Security Tag Type 4

Tag type 4 is the Security Level Tag Type. Tags of this type are used to label PDUs according to a hierarchical security level scheme. The set of possible values shall be ordered such that higher values indicate higher security levels. The set of possible values and the tag length are indicated in the CSOR.

5.3.5 Security Tag Type 5

Tag type 5 is the Free Form Tag Type. Tags of this type carry a free format field. This tag may hold character strings, or any other user-defined data. The entry registered in the CSOR shall indicate the format and interpretation for the information in this tag.

Appendix A: Standard Security Label Encoding for the Network and Transport Layers (Normative)

A.1 Local Acronyms and Definitions

LI - Acronym for Length Indicator.

- Length Indicator - This field indicates the length of the
- Security Information field of a label.
- Security Label Indicator field - This field identifies the
- information that follows as a security label.

Security Tag Length field - Gives the length in octets of the information in a tag.

- Security Tag Type field - Identifies which kind of tag follows.

TL - Acronym for Security Tag Length field.

- Tag Set Length field - Gives the length in octets of the security tag set that follows.

A.2 Security Label Format

Figure A.1 shows the security label format for use at the Network and Transport Layers. This figure identifies three fields:

Security Label Indicator, Length Indicator, and Registered Field Set.

ZDDDDDDDDDDDDDBDDDDDDDDDDDDDBDDDDDDDDDDDDDD?

3 Security 3 Length 3 Registered 3

3 Label 3 Indicator 3 Field Set 3

3 Indicator 3 3 3

3 C0 (hex) 3 3 3

@DDDDDDDDDDDDADDDDDDDDDDDDADDDDDDDDDDDDDDY

1 octet 1 octet Var

Security Label Format Layers 3 and 4

Figure. A.1

A.3 Security Label Indicator

- The size of the Security Label Indicator field is 1 octet. Its value is 1100 0000 (C0 hex).

A.4 Length Indicator

The size of the Length Indicator (LI) field is 1 octet. Its value is the total length of the Registered Field Set, Security Label Indicator, and Length Indicator in octets. The maximum value of the LI is 255.

A.5 Registered Field Set

One or more Registered Fields are carried in a single label. At this level, every Registered Field is an ordered set of the following: Tag Set Name Length, a Tag Set Name, Tag Set Length, and Security Tags. Figure A.2 depicts a Register Field.

ZDDDDDDDD Security Tag Set DDDDD?

ZDDDDDDDDDD?ZDDDDDDDDDD?ZDDDDDDDDDD?ZDDDDDDDDDDBDD D D D DDBDDDDDDDDDD?

3 Tag Set 33 Tag Set 33 Tag 33 Security 3 3 Security 3

3 Name 33 Name 33 Set 33 Tag 3 3 Tag 3

3 Length 33 33 Length 33 3 3 3

@DDDDDDDDDDY@DDDDDDDDDDY@DDDDDDDDDDY@DDDDDDDDDDA DD D D D DDADDDDDDDDDDY

1 octet Var 1 octet Var

Registered Field

Figure A.2

A.5.1 Tag Set Name Length

The size of the Tag Set Name (TSN) Length field is 1 octet. Its value is the length of the TSN in octets plus 1. The sum of the values of all the TSN Lengths and TSLs shall equal the value of the LI.

A.5.2 Tag Set Name

The Tag Set Name (TSN) is a variable-size field containing the value portion of the numerical object identifier for the label definition registered in the Computer Security Objects Register (CSOR). The Numeric Name assigned by the CSOR is encoded according to the Basic Encoding Rules (BER) [5] rules for Object Identifiers. The registered definition provides the semantics for the Security Tag Set in the Registered Field.

A.5.3 Tag Set Length

The size of the Tag Set Length (TSL) field is 1 octet. Its value is the total length, in octets, of the tags in the set plus 1.

This length field makes it possible to skip over an unrecognized Registered Field when scanning a label. The sum of the values of all the TSN Lengths and TSLs shall equal the value of the LI.

A.5.4 Security Tags

The security information is conveyed using Security Tags. The type, number, usage, and interpretation of the security tags are given by the CSOR. The Tag Set Name points to a label definition in the CSOR. Each Security Tag has one-octet type and length fields plus a variable size information field.

A.5.4.1 Security Tag Type

The size of the Security Tag Type field is 1 octet. Its value indicates the tag type. Values range between 0 and 255. This standard defines tag types 1 through 5. All other tag types are reserved for definition by NIST. At least one tag must be present in every Registered Field.

A.5.4.2 Security Tag Length

The size of the Security Tag Length (TL) is 1 octet. Its value is the length, in octets, of the information in the tag plus 2 (for the length of the Type and Length fields). Its value ranges between 2 and 250 octets. The sum of all the TL values in a Registered Field shall equal the value of the TSL.

A.5.4.3 Security Information

This variable length field contains the value of the Security Tag. This standard describes this field for Tag Types 1 - 5. All other tag types are reserved for later definition by NIST.

A.5.4.3.1 Security Tag Type 1

Security tags of this type carry a bit map of security attributes. The complete set of possible attributes is represented with the bit values off and on set as appropriate. The interpretation of bit values in a bit map is given by the CSOR.

Bits in the map shall be numbered starting with the most significant bit of the first transmitted octet (bit 0). Bit maps shall be padded to the right (i.e., up to the least significant bit of the last octet), if necessary.

The format of this tag type is as follows:

0123 ...

ZDDDDDDDDDDDDBDDDDDDDDDDDDBDDDDDDD D D DDDDDD?

3 00000001 3 LLLLLLLL 3 BBBB BBBB 3
@DDDDDDDDDDDDADDDDDDDDDDDDADDDDDDD D D DDDDDDY

Tag Type Tag Length Bit Map

Security Tag Type 1

Figure A.3

A.5.4.3.2 Security Tag Type 2

Tag Type 2 is used when only a few security attributes out of a large set need to be singled out for a PDU. This is done by enumerating the attributes that apply (set inclusion), or do not apply (set exclusion). This enumeration shall start with the lowest numbered attribute following an ascending order. Valid TL field values for this tag type are multiples of 2. The CSOR will indicate whether attributes enumerated in a type 2 tag will be interpreted as included or excluded from the applicable set.

A single tag may enumerate several security attributes, assigning 2 octets per attribute. The attributes enumerated may be between 0 and 65535.

The format of this tag type is as follows:

ZDDDDDDDDDDDDBDDDDDDDDDDDDBDDDDDDD D D DDDDDD?

3 00000010 3 LLLLLLL0 3 AA AA AA AA 3

@DDDDDDDDDDDDADDDDDDDDDDDDADDDDDDD D D DDDDDDY

Tag Type Tag Length Enumerated

Attributes

Security Tag Type 2

Figure A.4

A.5.4.3.3 Security Tag Type 3

Tag Type 3 is used when all the security attributes between certain lower and upper bound need to be singled out for a PDU. This is done by indicating the higher-numbered and lower-numbered attributes as bounds for the range. Valid length (TL) field values for this tag type are multiples of 2. The CSOR will indicate whether attributes in a range will be interpreted as included or excluded from the applicable set.

A single tag may indicate multiple security attribute ranges.

These ranges shall be listed in descending numerical order and shall not overlap. Each bound attribute is indicated by a 2-octet binary number. The final lower bound may be omitted if its value is 0. Security attributes are identified by integers between 0 and 65535.

The format of this tag type is as follows:

ZDDDDDDDDDDDDBDDDDDDDDDDDDBDDDDDD D D DDDDDD?

3 00000011 3 LLLLLLL0 3 UUUU DDDD 3
@DDDDDDDDDDDDADDDDDDDDDDDDADDDDDD D D DDDDDDY

Tag Type Tag Length Range Set

Security Tag Type 3

Figure A.5

A.5.4.3.4 Security Tag Type 4

Tag type 4 carries a security level indicator. Possible values are non-negative integers. The set of possible levels shall be assigned such that higher values indicate higher security levels. The set of possible values and the tag length are indicated in the CSOR.

The format of this tag type is as follows:

ZDDDDDDDDDDDDBDDDDDDDDDDDDBDDDDDD D D DDDDDD?

3 00000100 3 LLLLLLLL 3 SSSS SSSS 3
@DDDDDDDDDDDDADDDDDDDDDDDDADDDDDD D D DDDDDDY

Tag Type Tag Length Security Level

Security Tag Type 4

Figure A.6

A.5.4.3.5 Security Tag Type 5

Tag type 5 carries a free format field of up to 248 octets. The information field of this tag may hold character strings, or any user-defined data.

The format of this tag type is as follows:

ZDDDDDDDDDDDDBDDDDDDDDDDDDBDDDDD D D DDDDD?

3 00000101 3 LLLLLLLL 3 FFFF FFFF 3

@DDDDDDDDDDDDADDDDDDDDDDDDADDDDD D D DDDDDY
Tag Type Tag Length Free Form

Field

Security Tag Type 5

Figure A.7

A.6 Usage Rules

Throughout this appendix it is assumed that the leftmost bit is the most significant bit (MSB). The MSB, labeled bit 0, is always transmitted first. All illustrated fields are transmitted from left to right.