NISTIR 5308

General Procedures for Registering Computer Security Objects

Noel A. Nazario
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
National Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 5308

General Procedures for Registering Computer Security Objects

Noel A. Nazario
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
National Computer Systems Laboratory
Gaithersburg, MD 20899

December 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

General Procedures for Registering Computer Security Objects

Foreword

The National Institute of Standards and Technology is responsible, under the Computer Security Act of 1987, for the development of standards and guidelines to assure the cost-effective security and privacy of sensitive information in Federal computer systems. In meeting this responsibility, NIST promotes development of commercial products that meet Government security requirements for secure communication. The heterogeneous nature of existing Government systems highlights the need to adhere to standards to foster interoperability among communicating systems.

The use of standards alone does not insure interoperability. Implementations of specific standards may fail to interoperate because they support incompatible sets of options, accept different parameters, or employ incompatible mechanisms. For instance, security standards that rely on cryptographic algorithms to provide a confidentiality service do not usually specify what algorithm to use. Furthermore, some cryptographic algorithms have various modes of operation. To improve chances of interoperability, some implementations handle multiple options. Such implementations require that such options be unambiguously identified and agreed upon by the communicating parties before data can be securely exchanged. The use of a common source for specifications of these optional elements should further interoperability.

The elements referred to above are generically known as objects. A Computer Security Object (CSO) is the definition or representation of a resource, tool, or mechanism used to maintain a condition of security in computerized environments. This broad definition covers many elements referred to in standards that are either selected or defined by separate user communities.

NIST is establishing a register for CSOs to provide stable object definitions identified by unique names. The use of this register will enable the unambiguous specification of security parameters and algorithms to be used in secure data exchanges.

These "General Procedures for Registering Computer Security Objects" describe the object-independent procedures for operating the Computer Security Objects Register (CSOR). The CSOR services organizations and individuals seeking to use a common set of tools and techniques in the area of computer security. The procedures described herein follow guidelines for registration of the ISO/IEC Joint Technical Committee 1 (JTC1) and the American National Standards Institute (ANSI). The CSOR is not associated with a particular standard nor is it recognized by the ISO/IEC at the time of its establishment. In the future, however, NIST may turn the CSOR over to an organization recognized by the ISO/IEC for operation.

Initially, one family of objects will be registered in the CSOR: network security labels. Other families of security objects that eventually may be registered include cryptographic algorithm modes of operation, security association parameter sets, and authentication techniques. Procedures for registering specific families of objects appear as appendices to this document. Further details and additional appendices will be added by the registration authority as necessary and included in updates to this document.

Disclaimer

The registration service described in this document does not provide an endorsement or approval for techniques, algorithms, or products using the specifications maintained. Similarly, there is no explicit or implicit indication of the correctness or suitability of registered computer security objects for any use. Use of the Computer Security Objects Register (CSOR) is not mandatory, although recommended as a tool for achieving interoperability. Conflicts with ownership and/or rights over alpha-numeric object names and specifications must be resolved by applicants prior to the submission of a request for registration. The registration of a security object assigns the applicant no rights over the object or its name and is therefore no absolute proof of ownership. Registered objects and their names may be protected by copyrights and or patents and their use by others than the owner may require special arrangements without the involvement of the Registration Authority. Upon requesting registration, applicants give the Registration Authority permission to reproduce and distribute the names and specifications of all objects.

Table of Contents

General Procedures for Registering Computer Security Objects

1.0 Introduction

1.1 Purpose

Increasingly, the establishment and use of standards in the field of Open Systems Communications is based on the use of information objects that are unambiguously identifiable. To meet this requirement, ISO/IEC JTC1 has established a hierarchical structure (a tree) of Registration Authorities. This tree is the basis for a naming methodology that assures that an object may be unambiguously identified. Unique names are constructed by concatenating name components along the path from the root to the registered object. Each name component is guaranteed to be unique within each Registration Authority's structure.

ISO/IEC has designated the American National Standards Institute (ANSI) as the National Body organization to be the top level Registration Authority in the U.S. This document is based on the document, Procedures for Registering Organizational Names in the United States of America [1]. That document defines the procedures under which the U.S. Registration Authority operates.

The primary purpose of this register is to specify names that uniquely identify Computer Security Objects (CSOs). Unique names can be used to reference objects during the negotiation of security services for a transaction or application. The register is also a repository of parameters associated with the registered object.

Some CSOs cannot accommodate the size requirements of hierarchical names. Such CSOs require the use of fixed-length numeric names. To insure the uniqueness of numeric names assigned from such flat numbering space it is necessary to coordinate the assignment of names among the various registration authorities. The CSOR will provide such coordination by serving as the central clearing house for numeric names within shared numbering spaces.

1.2 Scope

This document defines the principles of operation for the CSO Registration Authority. It establishes the role and responsibilities of both the Registration Authority and the applicant. Specifically, the procedures outlined in this document:

(a) limit the role of this Registration Authority to an administrative role;

(b) describe the way in which applications for registration of Computer Security Objects are handled, including mechanisms for assuring the assignment of unique names at this level in the hierarchy;

(c) specify the syntax of names assigned by this Registration Authority;

(d) provide for the assignment of Computer Security Object names

1.3 Overview

The Registration Authority provides unique Computer Security Object (CSO) name values in two forms: numeric and alphanumeric. The Registration Authority generates the unique numeric name value. The unique value in the alphanumeric name form may be requested by the applicant, but is assigned by the Registration Authority. These two values are associated with the same object.

2.0 References

[1] ANSI Procedures for Registering Organizational Names in the United States of America, ISSB 989 Rev. 2, 1991.

[2] FIPS PUB 1-2 Code for Information Interchange, its Representations, Subsets, and Extensions, 1984.

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

[4] ISO/IEC JTC1 N820 Guidelines for Procedure Standards for JTC1 Registration Authorities, 1990.

3.0 Definitions and Abbreviations

3.1 Definitions

applicant:	An entity (organization or individual) that requests the assignment of a name from a Registration Authority [4].
computer security object:	Information object used to maintain a condition of security in computerized environments. Examples are: representations of computer or communications systems resources, security label semantics, modes of operation for cryptographic algorithms, and one-way hashing functions.

information object:	A well-defined piece of information, definition, or specification that requires a name to identify its use in an instance of communication [3].
name:	A unique identifier associated with a registered object. This register assigns two of names, a numeric name and an alpha-numeric name, to each object.
object identifier:	A value (distinguishable from all other such values) that is associated with an information object [3].
register:	A set of records (paper, electronic, or a combination) maintained by a Registration Authority containing assigned names and the associated information [4].
registration:	The assignment of a name to an object [4].
Registration Authority:	An organization approved by ISO/IEC for performing registration [4].

3.2 Abbreviations

ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One [3]
CSO	Computer Security Object
CSOR	Computer Security Objects Register
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JTC1	Joint Technical Committee 1
OSI	Open Systems Interconnection

4.0 Registration Authority

The Registration Authority (see Appendix A) maintains a register of Computer Security Objects known as the CSO Register. The Registration Authority assures that registration requests conform to the registration procedures. The Registration Authority, however, does not evaluate or make any judgement of the quality of protection provided by the registered object.

The Registration Authority performs the following functions:

(a) reviews, then accepts or rejects registration requests in accordance with the rules provided,

(b) assigns names to CSOs,

(c) adds or modifies register entries in accordance with the rules provided,

(d) provides copies of the register or information from the register.

5.0 Criteria for Eligibility

Any organization or individual (i.e., applicant), U.S. or foreign, may request the Registration Authority to register Computer Security Objects provided that the applicant demonstrates ownership or control of the object. Applicants are required to submit a written statement asserting their ownership or control over the CSO being registered. Ownership or control is obtained either by creating the object or through delegation by the creator or owner.

Although commercial products are not eligible for registration, CSOs used by such products may be registered. The CSOR will not register U. S. classified CSOs nor hold any classified information regarding registered objects.

6.0 Processing of Applications

This section specifies the Registration Authority's methods for processing registration requests. These processing guidelines are designed to assure openness and due process in the registration of name values.

6.1 Application for Registration

To request registration of a CSO, the applicant must submit a Request for Registration application and the appropriate registration fee to the Registration Authority. The content of this request is given in Appendix B. Object dependent information required for registration is outlined in Appendices C and D.

The applicant is required to provide a release statement giving the CSOR authorization to reproduce and distribute object information. Only information required for the correct implementation and handling of CSOs is registered; security policy-related procedures and guidelines for the usage of the objects are a local matter.

A registration fee must accompany all applications. This fee is used to defray the cost of operating the Registration Authority, and to discourage frivolous registration requests. If an application is rejected, the fee shall be returned minus any funds used for processing the application. (*See Section 9*)

6.2 Review of Application

An application for registration shall be reviewed as follows:

(a) The requested alphanumeric CSO name value will be compared against all previously registered or reserved names to assure a unique name value. *Note: Names may be reserved for sixty working days according to the procedure in Section 8.1.*

(b) Because a suggested alphanumeric CSO name value may have a meaning outside the registration process, there may be challenges concerning the rights to the name. Consequently, the registration application must contain a signed statement asserting the applicant's right to the object to be registered and to the requested name. If the statement is missing, the request will be rejected specifying the omission as the reason for rejection.

(c) If an application does not contain the minimum information specified in Appendix B, the application shall be rejected. The rejection notice will indicate the omission as the reason for rejection.

(d) If the requesting organization does not meet the criteria for eligibility specified in Section 5, the application shall be rejected. The rejection notice will indicate the failure to meet the criteria in Section 5 as the reason for rejection.

The contents of the Rejection of Application notice are specified in Appendix B. If the rejection is for reasons other than inability to demonstrate ownership, the applicant has ten working days from the date of rejection to submit any missing or incomplete information. Failure to submit the missing information during this period forfeits all fees and terminates the application process.

Each application is considered separately. Applications are reviewed for completeness and a written response regarding completeness shall be issued within ten working days from the date of receipt. This response consists of either a rejection for incompleteness or a statement indicating the status of the request. The Registration Request Acknowledgement described in Appendix B is used for this purpose.

Any possible appeals and objections shall be presented to the Registration Authority in writing within ten working days after the issue of the response eliciting the objection.

6.3 Assignment of CSO Names

The assignment of CSO Names is the result of the registration process. This action shall be reported to the applicant within thirty working days from the date of receipt of the application. The application process is concluded by issuing the Registration Notice described in Appendix B.

The registered CSO name is recorded as two values - numeric and alphanumeric. The numeric value is intended to be easily processed by computers and the alphanumeric value is intended to be easily used by people. The numeric name may, for instance, be used to index a database of objects recognized by a computer system. The alphanumeric name could be used in system specifications for procurement purposes.

The applicant shall not submit a numeric name value for registration. The Registration Authority shall assign a number with a unique value that shall not be assigned to any other object. The syntax of the numeric names is one of two types: ISO-defined object identifiers [3], or an unsigned fixed-length integer. The hierarchical syntax of object identifiers guarantees the uniqueness of the name. The use of unsigned integers as numeric names requires coordination among registration authorities to insure their uniqueness. The numeric name is an index to the registration database.

The applicant may supply an alphanumeric name value. Applicant-supplied alphanumeric names shall be variable length character strings of not less than one non-blank character, nor more than sixty four characters. The characters within the name strings must be taken from the 95-character graphic subset identified in FIPS PUB 1-2 [2]. For name comparison purposes, multiple spaces are equated to a single space and letter case differences will be ignored.

If the alphanumeric CSO name value does not meet the applicable syntax requirements the request shall be rejected specifying this as the reason for rejection. The supplied value shall be compared against all other alphanumeric values recorded in the registration database for that computer security object type. If the value is a duplicate, the request shall be rejected specifying duplication as the reason for rejection.

If the application is rejected, for either of the above reasons, the applicant shall be so notified. The contents of the Rejection of Application notice are specified in Appendix B. If the requested name is accepted, it shall be entered into the Register with the appropriate hierarchical identifier prefixed to it. This hierarchical prefix corresponds to the prefix for the numeric name.

7.0 Maintenance of the Register

The Registration Authority is responsible for defining its own internal methods. These methods include:

(a) mechanisms for maintaining the integrity and confidentiality of the registration database including adequate backup;

(b) the design of appropriate forms (paper, electronic or both), containing the data elements specified;

(c) a process for auditing the registration database and financial accounts;

(d) management of the object name space.

Ownership of a CSO name may be transferred. An official of the organization originally requesting registration of an object may request the Registration Authority to transfer ownership of the object and to update the register.

Once registered, neither the numeric value nor the alphanumeric name value can be deleted from the register. However, they can be marked as no longer valid upon request of the owner. The process is called de-activation and it requires a written request from the owner of the CSO. De-activation requests shall include a reason for de-activation and an optional pointer to a superseding CSO.

8.0 Supplemental Services

The services described below are optional and not an integral part of the Registration Authority Procedures.

8.1 Register Inquiry

An inquiry service is available from the Registration Authority that allows potential applicants to determine if a name has already been registered. This saves the cost of submitting an Application for Registration specifying a CSO name that is already registered. If the name is not registered it is reserved for the originator of the inquiry for sixty working days.

To make an inquiry, an organization shall submit an Inquiry Request to the Registration Authority containing the data elements specified in Appendix B. The request shall be accompanied by an inquiry fee (see Section 9.2).

The Registration Authority shall respond to such an inquiry within ten working days of the receipt of the inquiry (as described in Appendix B).

8.2 Register Publication

A publication service is available to provide hard copies of the CSO Register for specific object types. Single copies or one-year subscriptions may be purchased. Every copy contains all registered information on a specific CSO type. Change pages will be issued to all subscription holders as new objects are added. In addition the CSOR shall be available on-line at no cost.

9.0 Fees

The fee structure is designed to recover the expenses of operating as a Registration Authority and to discourage frivolous and multiple requests. Information on the types of fees, method of payment and their amounts in United States dollars can be obtained from the Registration Authority (*See* Appendix A).

9.1 Registration Fee

The registration fee shall be submitted along with the Request for Registration. This fee varies according to the object being registered. The Registration Authority reserves the right to change or waive the registration fee.

9.2 Inquiry Fee

The inquiry fee is included by the applicant with the inquiry request. The Registration Authority reserves the right to change or waive the inquiry fee.

9.3 Publication Fee

The publication fee for one-time copies and yearly subscriptions is established by the Registration Authority according to the size of the volume. The Registration Authority reserves the right to change or waive the publication fee.

APPENDIX A - REGISTRATION AUTHORITY

Computer Security Objects Register

National Institute of Standards and Technology
Computer Systems Laboratory
Program Coordination and Support Group
Building 225, Room B151
Gaithersburg, Maryland 20899
Telephone: (301) 975-2821
Facsimile: (301) 948-1784

APPENDIX B - INFORMATION REQUESTS AND NOTICES

This appendix defines the information requests and notices used by the Registration Authority.

B.1 Request for Registration Application

The Request for Registration shall contain the following information:

(a) name of the applicant;

(b) address of the applicant;

(c) name, title, address, telephone, and facsimile number of the point of contact for the applicant;

(d) statement on the releasability of the registered information (if applicable);

(e) statement asserting the ownership or control of the CSO for which registration is being requested and the rights over the proposed alpha-numeric name;

(f) object-specific registration information (*See appendices*).

B.2 Registration Application Acknowledgement

The Registration Application Acknowledgement shall contain the following information:

(a) name of the applicant;

(b) address of the applicant;

(c) name, title, address, telephone, and facsimile number of the point of contact for the applicant;

(d) status of the Request for Registration.

B.3 Rejection of Application Notice

The Rejection of Application Notice shall contain the following information:

(a) name of the applicant;

(b) address of the applicant;

(c) name, title, address, telephone, and facsimile number of the point of contact for the applicant;

(d) requested alphanumeric CSO name value - if supplied;

(e) stated reason for rejection.

B.4 Registration Notice

The Registration Notice is used to inform the applicant of the values that have been assigned and registered. This notice must be certifiable as authentic (e.g., a notary seal for paper, use of non-repudiation techniques for electronic messaging). It shall contain the following information:

(a) name of the applicant;

(b) address of the applicant;

(c) name, title, address, telephone, and facsimile number of the point of contact for the applicant;

(d) assigned numeric CSO name;

(e) assigned alphanumeric CSO name.

B.5 Inquiry Request

The Inquiry Request will contain the following information:

(a) name of the inquiry originator;

(b) address of the inquiry originator;

(c) name, title, address, telephone, and facsimile number of the point of contact for the inquiry originator;

(d) queried alphanumeric CSO name.

B.6 Inquiry Response

This Inquiry Response will contain the following information:

(a) name of the applicant;

(b) address of the applicant;

(c) name, title, address, telephone, and facsimile number of the point of contact for the applicant;

(d) queried alphanumeric CSO name value;

(e) status of the queried alphanumeric CSO name (e.g., already in use or not in use).

APPENDIX C - REGISTRATION REQUIREMENTS FOR SECURITY LABELS

This appendix outlines object-specific registration procedures for security label Named Tag Sets as defined by FIPS ___ - Standard Security Label for the Government Open Systems Interconnection Profile (SSL). Object-specific registration procedures indicate details that must be provided to register CSOs of a certain type. The required information is limited to details necessary to implement correctly the objects. The information outlined in this appendix shall be included with the Request for Registration Application specified in Appendix B of this document.

Register Fields are associated with local security policy, therefore policy-driven handling instructions and system responses to potential security events should be included in the registration information. The rationale for the handling instructions imposed and the meaning of the security information to the end system are local matters not to be included with the Request for Registration Application.

C.1 Required Information

C.1.1 Applicant Information

Applicant name: _____
Point of contact: _____
Date: _____

C.1.2 General Tag Set Information

Tag Set Name Format:

[ ] Object Identifier (Layer 7 label syntax)
[ ] Unsigned Integer (Layer 3 label encoding)

Requested Alpha-Numeric Name: _____

Maximum number of security tags: _____
Minimum number of security tags: _____
Tag combination and ordering rules: _____
_____
_____

C.1.3 Tag-Specific Information

For each tag indicate:

Tag number: _____Is order significant? _____(Yes/No)

Tag Type: _____ Is tag Optional or Mandatory?

List of valid attribute values: _____

The table format in the following example may be used to describe each tag. TT stands for tag type and TL is the tag length. The types are given in the SSL document. Only the tag values indicated will be accepted by an implementation of the Tag Set. An optional mnemonic may be associated to the each attribute value, bit, or field on the tag. A default value for each tag may be given, if appropriate. An optional tag order indication within the set also may be given. The presence of the tag in the set may be marked mandatory or optional. A Tag Set that does not match the format associated with the Tag Set Name preceding it is in error and shall be treated as such by the implementation.

TT	TL	VALUE	MNEMONIC (Optional)	DEFAULT VALUE	ORDER	M/O
01	01	(Security Level)			N/A	M
		11011011	CRITICAL	00000000		
		10101010	RESTRICTED			
		01010101	PROTECTED			
		00100100	GENERIC			
		00000000	unmarked			
		(Bits)				
		B16, 1	FOR-OFFICIAL-USE-ONLY	0 (May be omitted if all bits are 0)		
		B15, 1	CERTIFIED-COPIES-ONLY			
		B14, 1	DO-NOT-COPY			
		B13, 1	TIME-SENSITIVE			
		.				
		.				
		.				
		B01, 1	PROPRIETARY			

C.1.4 Security Object Usage Rules and Handling Instructions

This section shall cover object usage rules, handling instructions, and implementation details or restrictions beyond those imposed by the base standard. The text in this section may be used to clarify security tag information appearing in the Format Table. Examples are error conditions and their required system response such as return of an error response and local event auditing. The processing rules in Appendix B of the Standard Security Label FIPS may be referenced in this section. Explicit omissions, additions, or refinements to the processing rules in the SSL document also must appear in this section.

C.2 Security Tag Registration Rules

C.2.1 Special Rules for Bit Map Tags

1. Bit maps are defined to include integer multiples of eight bits.

2. All bits are numbered starting with one up to some upper bound, U, that follows the previous rule.

3. Bits not included in the bit map tag definition that fall between 1 and U are reserved and should not be used. The value for these bits is set to the default value indicated.

C.2.2 Special Rules for Enumerated Tags

1. The registration entry must specify whether the security attributes specified are to be included or excluded from the set of attributes that apply to the data unit.

2. If it were necessary to explicitly single out attributes for both inclusion and exclusion, they must appear in separate tags. To make the distinction, tag order shall be used.

C.2.3 Special Rules for Range Tags

1. The registration entry must specify whether the security attributes in the specified range(s) are to be included or excluded from the set of attributes that apply to the data unit.

2. If it were necessary to explicitly single out ranges for both inclusion and exclusion, they must appear in separate tags. To make the distinction, tag order shall be used.

C.2.4 Special Rules for Free Form Tags

1. The unspecified nature of this tag requires that both the syntax and semantics be explicitly stated.

2. For this and all tag types, the distinction between tags of the same type with different interpretations is based on the relative order of the tags.

APPENDIX D - OBJECT-SPECIFIC REGISTRATION INFORMATION

This appendix is a place holder for the Registration Authority to provide additional object-specific registration procedures. Appendices will be added to these general procedures for each CSO family to be registered. Object-specific registration requirements indicate the list of technical details that must be provided in order to register objects of that type. The required information will be limited to details necessary to implement correctly the object.