

ANNEX CDIRECTORY PROFILES1. General

This annex describes the ISPs that have been developed for the directory standards. This annex has been included in ACP 133 as background information on the functional profiles that provide the basis for the ACP 133 Profiles in Annex D. All profile requirements for the Allied Directory System are contained in Annex D.

a. Functional profiles are used to define the detailed capabilities of directory products. They are developed from the Directory Standards, in particular, the Protocol Implementation Conformance Statement (PICS) proformas, and refine these specifications by making choices where alternatives are defined and by setting specific values for parameters of directory protocol operation or directory information definition. For example, a profile could be written for a DUA product that limits the operations used to Bind, Unbind, and Read and restricts the attributes that are read to a certain set.

b. The directory functional profiles fall into two major categories: Application Profiles and Interchange Format and Representation Profiles. These categories are defined in ISO/IEC Technical Report (TR) 10000 which defines and classifies functional profiles for OSI. For the Directory, protocols and operations are the subjects of Application Profiles, and generic and application-specific schema are the subjects of Interchange Format and Representation Profiles. Within these two categories, the capabilities of the standard directory have been divided into several subject areas for profiling. Each subject area or class may be broken down further into functional profiles. Figure C-1 shows the directory functional profiles and the label applied to each one through the identification scheme (taxonomy) contained in TR 10000.

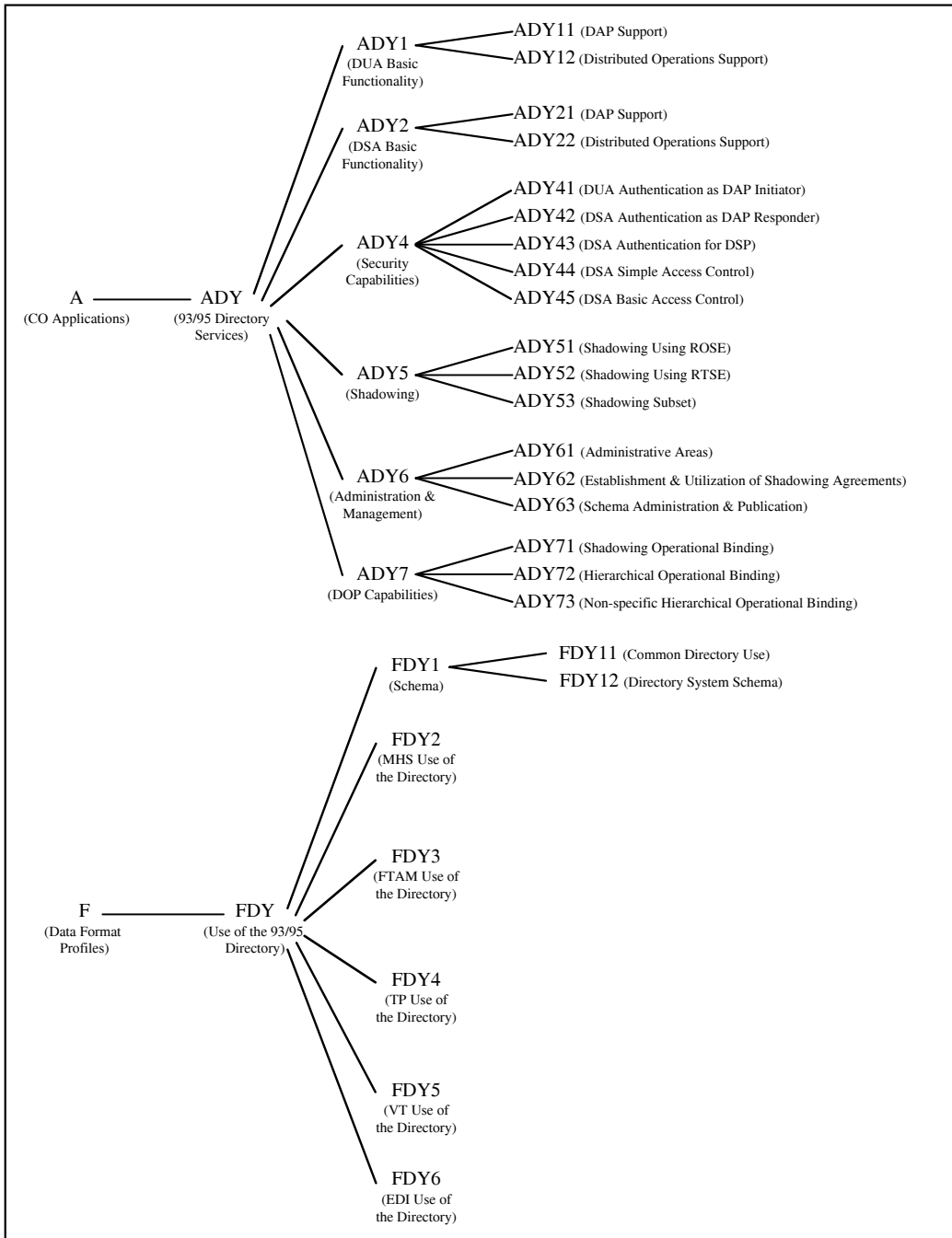


Figure C-1

Taxonomy of Directory Functional Profiles

- c. The classes of directory profiles are:
- ADY1 - DUA Basic Functionality
  - ADY2 - DSA Basic Functionality
  - ADY4 - Security Capabilities
  - ADY5 - Shadowing Capabilities
  - ADY6 - Directory Administration and Management
  - ADY7 - DOP Capabilities
  - FDY1 - Schema
  - FDY2 - MHS Use of the Directory
  - FDY3 - FTAM Use of the Directory
  - FDY4 - TP Use of the Directory
  - FDY5 - VT Use of the Directory
  - FDY6 - EDI Use of the Directory

2. Directory Application Profiles

a. ADY1 - DUA Basic Functionality

The ADY1 class of profiles defines the basic behavior of a DUA in its communication with a DSA. It does not define the DUA's interaction with the user. There are two functional profiles in this class:

- ADY11 - DUA Support of Directory Access Protocol
- ADY12 - DUA Support of Distributed Operations

(1) The ADY11 profile defines the behavior of a DUA regarding the operation of the DAP when interacting with a single DSA to perform a single user request. It covers the DUA performing the initiator role of DAP, invoking an operation on a DSA, and receiving a result or error response (see Figure C-2). ADY11 specifies constraints on the use of a DSA by a DUA to interwork with the Directory services.

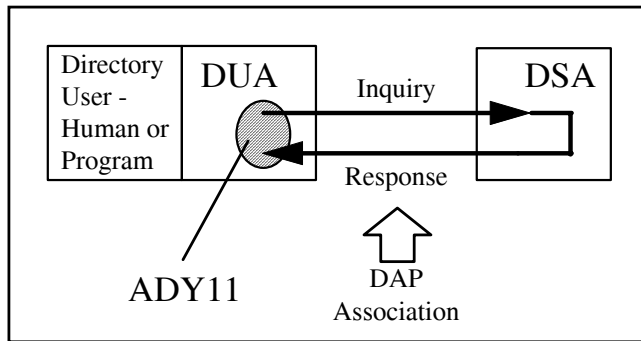


Figure C-2

## ADY11 Applicability

(2) The ADY12 profile defines the behavior of a DUA, regarding the operation of DAP, when performing multiple interactions with multiple DSAs to perform a single user request. That is ADY12 profiles the behavior of a DUA when Referrals or Search Continuation References are used by the Directory. A DUA creates an association to a DSA of its choice, and requests an operation. The DSA may return a referral instead of a result, or the result may contain continuation references. The latter occur in the case of List or Search operations in which the DSA is unwilling or unable to complete the search, but is able to advise which other DSAs may be able to assist. The DUA then associates with the recommended DSA to continue the operation. See Figure C-3.

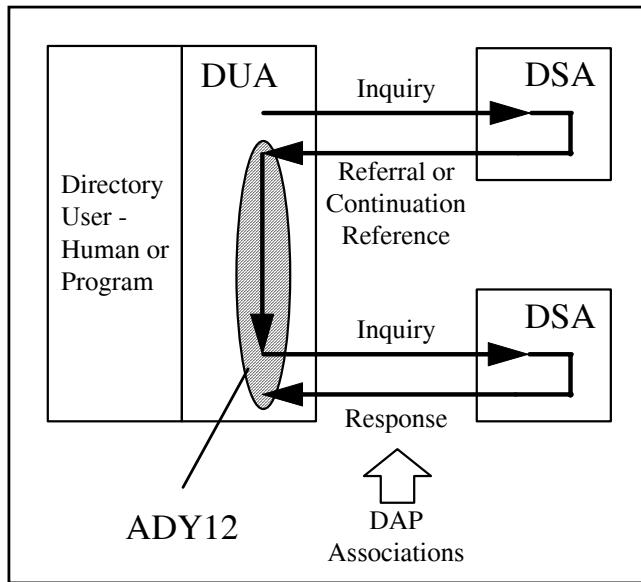


Figure C-3

## Applicability of ADY12

b. ADY2 - DSA Basic Functionality

The ADY2 class of profiles defines the basic behavior of a DSA in its communication with DUAs and other DSAs. There are two functional profiles in this class:

- ADY21 - DSA Support of Directory Access
- ADY22 - DSA Support of Distributed Operations

(1) The ADY21 profile defines the behavior of a DSA regarding the operation of the DAP for communicating with a DUA. It covers the DSA performing the responder role of DAP, receiving the invocation of an operation from a DUA, and responding with a result or error response (see Figure C-4). ADY21 defines capabilities and constraints on support for DAP by DSAs so that DUAs are able to interwork with the Directory.

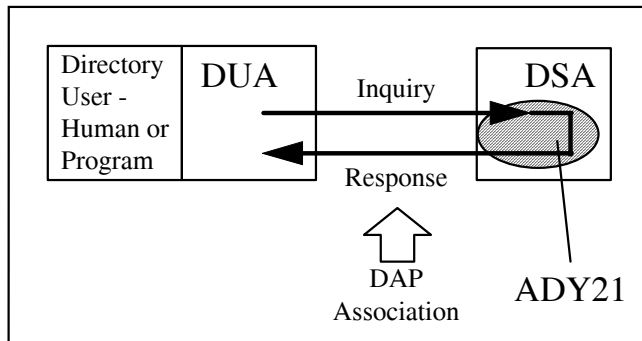


Figure C-4

## ADY21 Applicability

(2) The ADY22 profile defines the behavior of a DSA regarding the operation of the DSP when communicating with another DSA, and it defines the coordination of a DSA communication across several associations to perform a particular distributed operation (see Figure C-5). It covers the DSA performing the invoker role of DSP, the performer role, or both; DSAs as users (over DAP or DSP) of Referrals and Continuation references; and DSAs as users of Hierarchical Operational Bindings (HOBs) and of Shadow Operational Bindings in so far as they affect distributed operations using DSP. ADY22 ensures that DSAs will be able to interwork within the Directory in two respects:

- Correct protocol behavior
- Correct behavior in respect of the role that each DSA has to play in respect of Distributed Operations

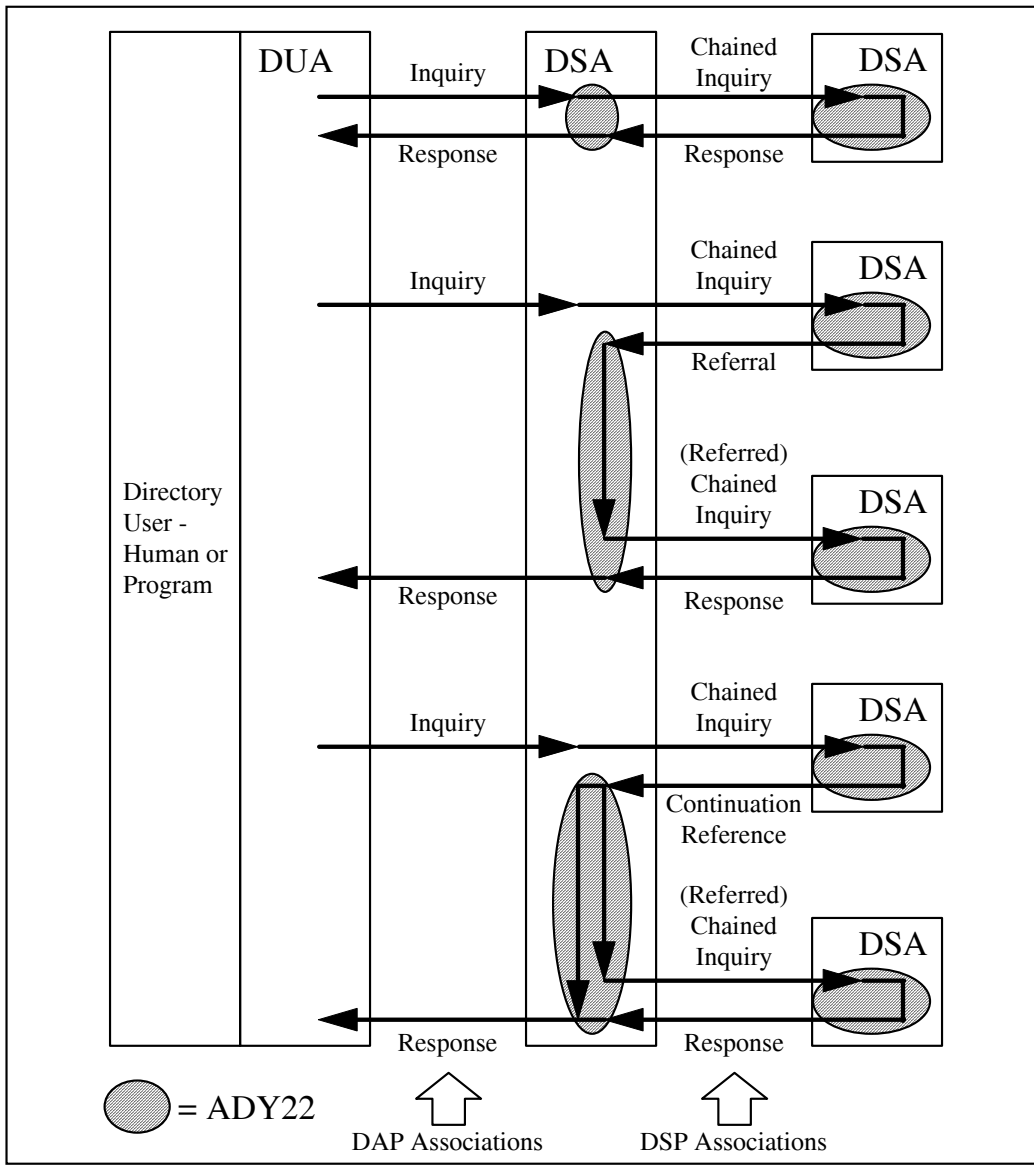


Figure C-5  
ADY22 Applicability

c. ADY4 - Security Capabilities

The ADY4 class of profiles defines the behavior of directory components in supporting various security features and degrees of security. There are five functional profiles in this class:

- ADY41 - DUA Authentication as DAP Initiator
- ADY42 - DSA Authentication as DAP Responder
- ADY43 - DSA to DSA Authentication
- ADY44 - DSA Simple Access Control
- ADY45 - DSA Basic Access Control

(1) The ADY41 profile specifies the manner in which a DUA behaves when authenticating a DSA and authenticating itself to a DSA using simple protected authentication or strong authentication as a DAP Initiator. It augments the ADY11 requirements with DUA-specific use of authentication beyond simple unprotected binds and use of digitally signed operations (see Figure C-6). ADY41 includes use of different levels of authentication, and of different security infrastructures, e.g., support of hierarchical/non-hierarchical CA structures. In addition, ADY41 covers actions by the DUA on handling (i.e., validating or not) credentials returned by the DSA, the use of two-way strong authentication, and digitally signed operations.



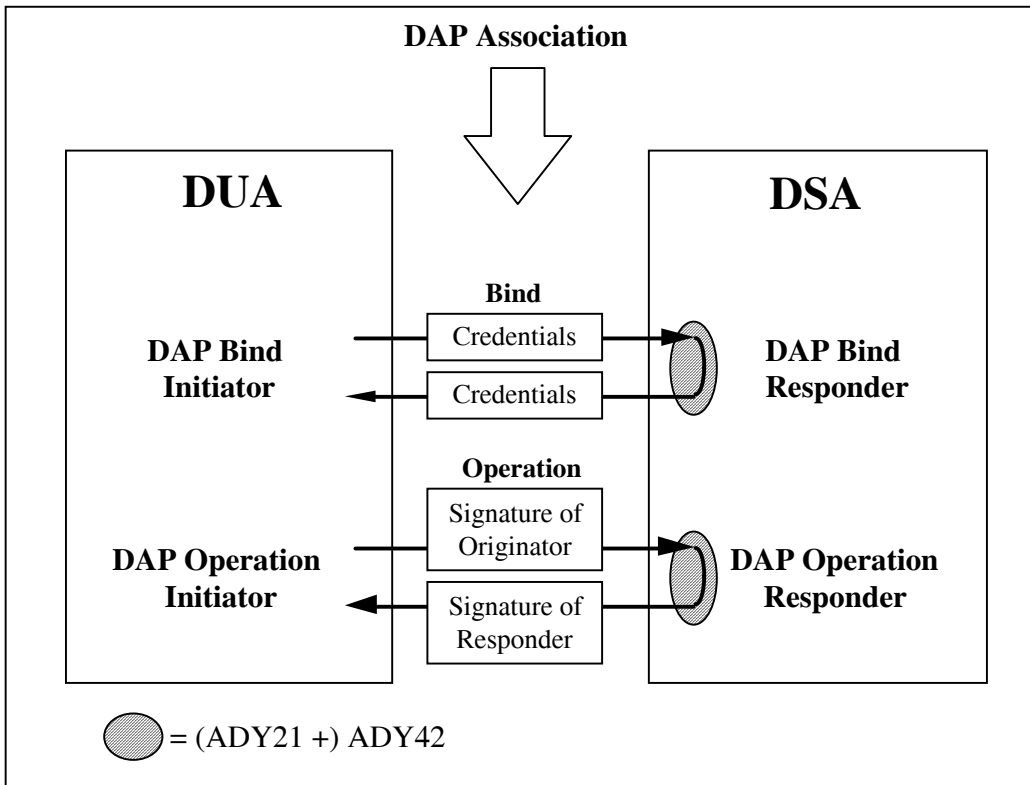


Figure C-7

## ADY42 Applicability

(3) The ADY43 profile is titled DSA to DSA Authentication. However, this is different from the title given in TR 10000 (DSA Authentication for DSP) and reflects a broadening of scope since the Directory profiles taxonomy was formulated. ADY43 covers the use of authentication beyond simple unprotected password for the purpose of mutual authentication of DSAs in establishment of DSP, DISP, and DOP associations. It includes use of 2 x one-way strong authentication, two-way strong authentication and the use of security-related protocol elements. ADY43 also covers digitally signed DSP and DISP operations. ADY43 profiles the behavior of a DSA in combining signed uncorrelated list and search information as returned by DSP return results and the use of the originator element to convey information about the originator of the DAP operation that is the cause of the DSP operations. See Figure C-8.

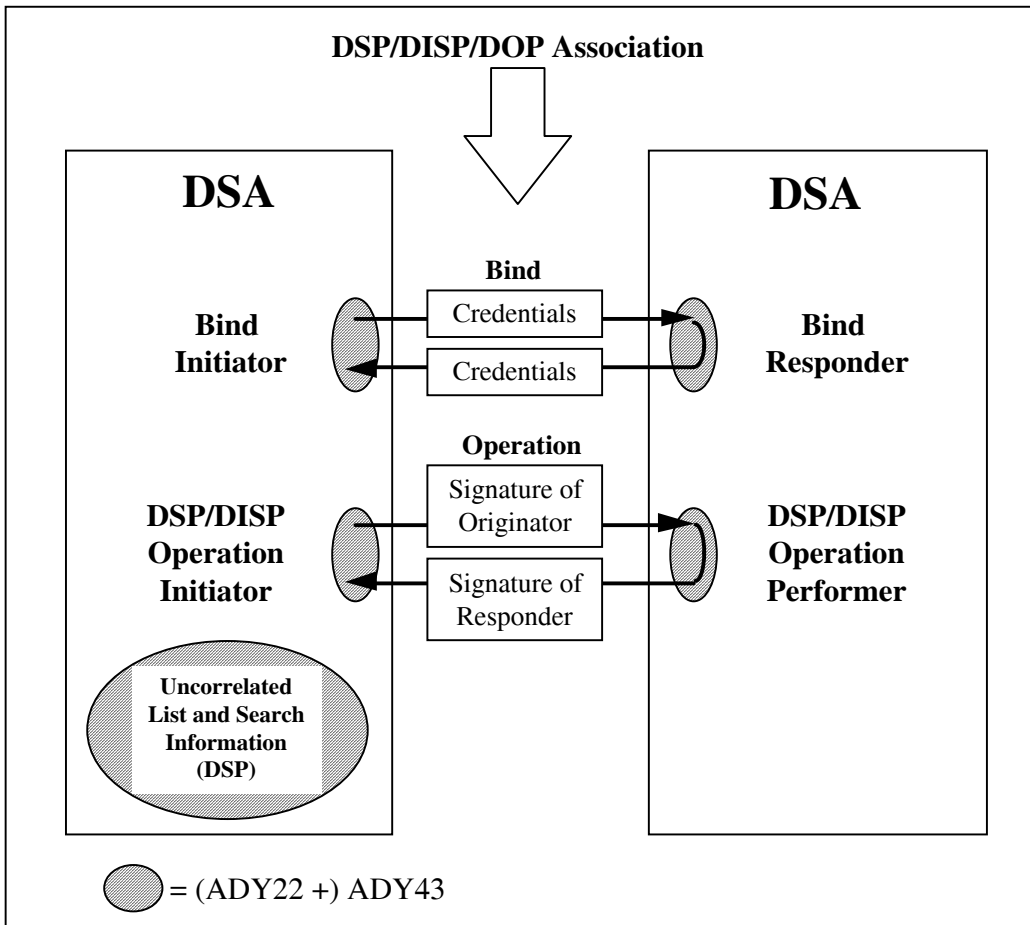


Figure C-8

## ADY43 Applicability

(4) Although ADY44 is defined in TR 10000 to be a separate profile from ADY45, ADY44 has been absorbed into ADY45, because of the large amount of commonality. The ADY44 profile specifies the manner in which DSAs perform Simplified Access Control (SAC) by supporting Access Control Specific Administrative Areas, Protected Item categories, User Classes, and GrantAndDenials facilities as defined in subentries. ADY44 defines capabilities and constraints of DSAs supporting SAC. SAC is performed by DSAs to determine if a requestor is allowed access to the requested information stored in the DSA. The DSA compares a presented DAP or DSP request for information to the stored information's ACIItem, and then performs an access control decision to determine whether permission to access the information should be granted or denied to the requestor (see Figure C-9). SAC is relevant both when the DSA is acting as responder to DAP requests from a DUA and as responder to DSP operations from a peer DSA. In SAC, access control decisions are made on the basis of ACIItem values of

prescriptiveACI and subentryACI operational attributes, which must be located at a single Administrative Point or its immediate subentries.

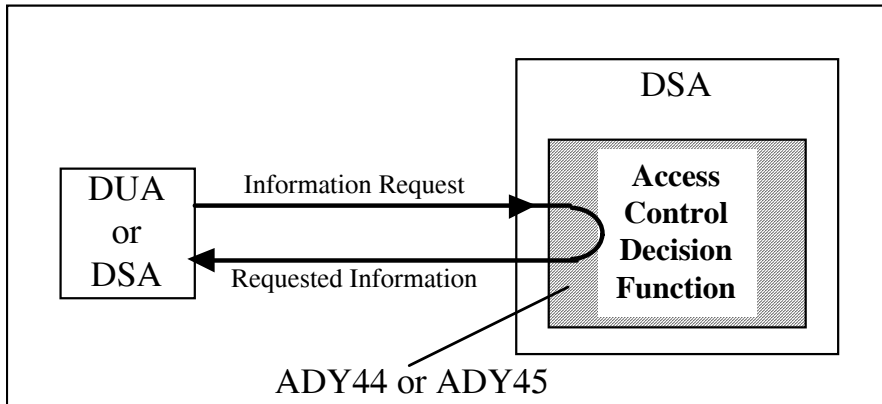


Figure C-9

## ADY44 or ADY45 Applicability

(5) The ADY45 profile specifies the manner in which DSAs BAC by supporting Access Control Specific Administrative Areas and Inner Administrative Areas, Protected Item categories, User Classes, and GrantAndDenials facilities as defined in subentries and/or entries. ADY45 defines capabilities and constraints of DSAs supporting BAC. BAC is performed by DSAs to determine if a requestor is allowed access to the requested information stored in the DSA. The DSA compares a presented DAP or DSP request for information to the stored information's ACItem, and then performs an access control decision to determine whether permission to access the information should be granted or denied to the requestor (see Figure C-9). BAC is relevant both when the DSA is acting as responder to DAP requests from a DUA and as responder to DSP operations from a peer DSA. In BAC, access control decisions are made on the basis of ACItem values of prescriptiveACI, subentryACI, and entryACI operational attributes. PrescriptiveACI and subentryACI are associated with the administrative point of an Access Control Specific Area or an Access Control Inner Area. EntryACI is associated with a particular entry.

d. ADY5 - Shadowing Capabilities

The ADY5 class of profiles covers the protocol and functional aspects related to Directory shadowing. Operational and procedural aspects of shadowing are covered in ADY22 and ADY62. There are three functional profiles in this class:

- ADY51 - Shadowing Using ROSE
- ADY52 - Shadowing Using RTSE
- ADY53 - Shadowing Subset

(1) The ADY51 profile defines a set of capabilities and constraints on support of DISP by DSAs when operating DISP over the Remote Operations Service Element (ROSE). ADY51 specifies a level of DISP capability such that DSAs shall be capable of establishing and maintaining DISP associations over ROSE together in a consistent manner. ADY51 covers primary and secondary shadowing and the consumer and supplier DSA roles.

(2) The ADY52 profile defines a set of capabilities and constraints on support of DISP by DSAs when operating DISP over the Reliable Transfer Service Element (RTSE). Both the consumer and supplier roles and the 'push' and 'pull' models are covered. In addition, error handling and recovery capabilities are also profiled.

(3) The ADY53 profile defines an incremental set of Directory shadowing capabilities that can be provided by a DSA implementation. These functional capabilities are related specifically to the level of refinement supported for the definition of a unit of replication. The capability to support overlapped units of replications is also incorporated. Both the DSA shadow supplier and consumer roles are covered.

e. ADY6 - Directory Administration and Management

The ADY6 class of profiles is aimed at regulating the policies and procedures that administrations shall define in order to make the Directory work smoothly in its environment. This is achieved by describing the various subjects for coordination within and between administrative areas and methods for the coordination based on derived policies. There are three functional profiles in this class:

- ADY61 - Administrative Areas
- ADY62 - Establishment and Utilization of Shadowing Agreements
- ADY63 - Schema Administration and Publication

(1) The ADY61 profile describes how administrative areas must be set up and subdivided into manageable portions, and ways in which the operation of the Directory and of the administrative areas are optimized through coordination of knowledge distribution, authentication and access control policies, distribution of naming contexts, etc. The use of quality requirements and resulting policies shall be the basis for the coordination procedures.

(2) The ADY62 profile describes how the initial phase of establishing a shadowing agreement shall be conducted for smooth introduction and utilization of the shadowing itself, and in addition, how the organizational management of such agreements shall be conducted, up to and including their dissolution.

(3) The ADY63 profile specifies how an administrative area shall administrate and publish its schema so that other administrative areas can be informed about the schema rules in use by the publishing area.

f. ADY7 - DOP Capabilities

The ADY7 class of profiles specifies the capabilities of a DSA for the using DOP facility to manage operational bindings. There are three functional profiles in this class:

- ADY71 - Shadowing Operational Binding
- ADY72 - Hierarchical Operational Binding
- ADY73 - Non-specific Hierarchical Operational Binding

(1) The ADY71 profile specifies how DOP is used by DSAs to establish, modify, and terminate shadow operational bindings in order to manage the standardized aspects of shadowing agreements.

(2) The ADY72 profile specifies how DOP is used by DSAs to establish, modify and terminate HOBs in order to manage the relationship and promulgate relevant information between two master DSAs. The DSAs hold naming contexts where one is immediately subordinate to the other and the superior DSA holds a subordinate reference to the subordinate DSA.

(3) The ADY73 profile specifies how DOP is used by DSAs to establish, modify and terminate Non-specific HOBs in order to manage the relationship and promulgate relevant information between two master DSAs. The DSAs hold naming contexts where one is immediately subordinate to the other and the superior DSA holds a non-specific subordinate reference to the subordinate DSA.

### 3. Directory Information Format and Representation Profiles

#### a. FDY1 - Schema

The FDY1 class of profiles specifies the Directory information that is common to a variety of applications. The Directory information covered includes both user information (placed in the Directory by, or on behalf of, users) and administrative and operational information (held and managed by the Directory to meet various administrative and operational requirements). There are two functional profiles in this class:

- FDY11- Common Directory Use
- FDY12 - Directory System Schema

(1) The FDY11 profile covers user information to be stored within the Directory that is common to a variety of applications. FDY11 defines the minimum capabilities that a DUA and a DSA shall support in order to share a basic common view of the Directory user information. It does this by specifying a minimum set of object classes, attribute types, name forms, structure rules and matching rules to be supported.

(2) The FDY12 covers administrative and operational information a DSA shall hold to operate properly. It includes support of schema for the administrative and operational information model, schema for access control, and schema for collective attributes. FDY12 defines the minimum capabilities that a DUA and a DSA shall support in order to share a basic common view of the Directory administrative and operational information. It does this by specifying a minimum set of requirements concerning the specific tree structure for operational information and the operational content of the entries and subentries.

#### b. Application-Specific Directory Functional Profiles

(1) There are five applications that have functional profiles defined for Directory information and schema aspects that are required by the application:

- FDY2 - MHS Use of the Directory
- FDY3 - FTAM Use of the Directory
- FDY4 - TP Use of the Directory
- FDY5 - VT Use of the Directory
- FDY6 - EDI Use of the Directory

(2) Of these profiles, FDY2, MHS Use of the Directory, is applicable to components of the Allied Directory System. However, a complete FDY2 does not exist yet. In the future, FDY6, EDI Use of the Directory may be required.

(3) The FDY2 profile defines Directory user information concerning MHS that is needed in addition to the common information defined in FDY11. FDY2 defines the minimum capabilities that DSAs must have to support an MHS application's view of Directory information. It does this by specifying a minimum set of structure and naming elements for the DIT which a DSA must be capable of holding and accessing, and other minimum schema requirements.

#### 4. Directory ISPs

Standard functional profiles are published in a type of document ISP. One or more functional profiles can be published in one ISP. As can be seen in Figure C-10, the directory Application Profiles are contained in one ISP that has a separate part corresponding to each functional profile. The generic directory Information Format and Representation Profiles are also contained in a multi-part ISP. However, each of the application-specific directory functional profiles is contained in a separate ISP.

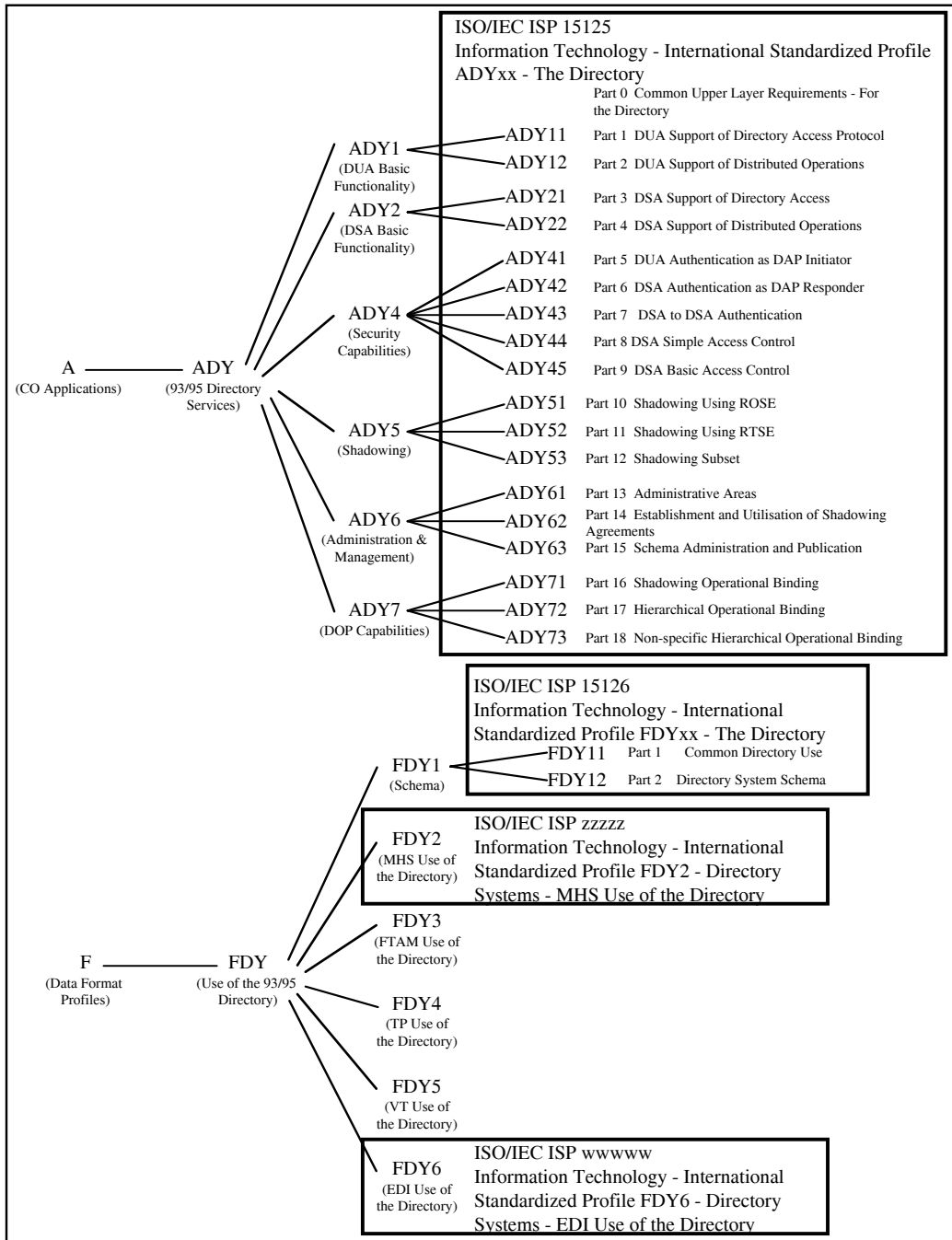


Figure C-10

Organization of Directory Functional Profiles Into International Standardized Profiles



ANNEX D

ALLIED DIRECTORY SYSTEM FUNCTIONAL PROFILES

TABLE OF CONTENTS

SECTION I

INTRODUCTION

1. General..... D-1

SECTION II

ACP 133 ADDITIONS TO CURRENT ISPS AND PICS

2. Schema..... D-1  
    a. Common Content..... D-1  
    b. Allied Directory System Schema..... D-4  
3. DUAs ..... D-5  
4. DSAs..... D-12  
    a. DAP..... D-12  
    b. DSP..... D-16  
    c. DISP..... D-20  
    d. DOP..... D-22

SECTION III

DUA EXTENSIONS

5. Administrative DUAs ..... D-24

SECTION IV

ACP 133 PROTOCOL AND SCHEMA EXTENSIONS

6. Common Content Extensions ..... D-26  
    a. Object Classes..... D-26  
    b. Attribute Types ..... D-29  
    c. Name Forms..... D-36  
    d. Matching Rules ..... D-38  
7. DUA Extensions ..... D-38  
    a. General..... D-38  
    b. AddEntryResult ..... D-39  
    c. RemoveEntryResult ..... D-40  
    d. ModifyEntryResult ..... D-40  
    e. ModifyDNResult ..... D-41  
    f. Errors ..... D-42  
    g. Security Parameters ..... D-44

8. DSA Extensions .....	D-45
a. DAP.....	D-45
b. DSP .....	D-46
c. DISP .....	D-47
9. Schema Extensions .....	D-49
10. Corrigenda not included in ISPs .....	D-49

## List of Tables

Table D-1: Identification of the Implementation and/or System - Single DSA .....	D-2
Table D-2: Identification of the Implementation and/or System - DUA.....	D-3
Table D-3: X.520 Collective Attribute Types .....	D-3
Table D-4: Standard Matching Rules .....	D-4
Table D-5: Identification of the Implementation and/or System - Single DSA .....	D-5
Table D-6: Standard Operational Attribute Types - DSA Support.....	D-5
Table D-7: Operations .....	D-6
Table D-8: Extensions .....	D-6
Table D-9: Service Controls .....	D-7
Table D-10: Entry Information Selection.....	D-7
Table D-11: General Capabilities .....	D-7
Table D-12: Supported Security Levels.....	D-8
Table D-13: Directory Bind Arguments .....	D-8
Table D-14: Security Parameters.....	D-9
Table D-15: General Security .....	D-10
Table D-16: Strong Authentication.....	D-10
Table D-17: Signed Operations .....	D-12
Table D-18: General Capabilities .....	D-12
Table D-19: Operations .....	D-13
Table D-20: General Capabilities .....	D-13
Table D-21: Supported Security Levels.....	D-13
Table D-22: General Security .....	D-14
Table D-23: Strong Authentication.....	D-14
Table D-24: Signed Operations .....	D-15
Table D-25: Supported Access Control Schemes.....	D-15
Table D-26: Access Support .....	D-15
Table D-27: DSA implementation and/or system.....	D-16
Table D-28: Global Statement of Conformance - DSP .....	D-18
Table D-29: Global Statement of Conformance - DSP, DOP, DISP.....	D-18
Table D-30: General Capabilities .....	D-19
Table D-31: Supported Access Control Schemes.....	D-19
Table D-32: Access Support.....	D-20
Table D-33: Global Statement of Conformance - DISP .....	D-20
Table D-34: Global Statement of Conformance .....	D-21
Table D-35: DSA Implementation.....	D-22
Table D-36: Global Statement of Conformance - DOP.....	D-22

Table D-37: Summary of Support .....	D-23
Table D-38: Identification of the Implementation and/or System - Administrative DUA.....	D-24
Table D-39: Standard Operational Object Classes - Administrative DUAs.....	D-24
Table D-40: Standard Operational Attribute Types - Administrative DUAs .....	D-25
Table D-41: X.402 Object Classes .....	D-27
Table D-42: ACP 133 Object Classes.....	D-27
Table D-43: 1997 Standard Object Classes .....	D-28
Table D-44: X.509(1997) DAM 1 Standard Object Classes .....	D-29
Table D-45: X.402 Attribute Types .....	D-29
Table D-46: ACP 133 Attribute Types .....	D-30
Table D-47: RFC 1274 Attribute Types .....	D-35
Table D-48: 1997 Standard Attribute Types.....	D-35
Table D-49: ACP 133 Collective Attribute Types.....	D-36
Table D-50: ACP 133 Name Forms .....	D-36
Table D-51: 1997 Standard Name Forms .....	D-37
Table D-52: 1997 Standard Matching Rules .....	D-38
Table D-53: 1997 Security Enhancements .....	D-39
Table D-54: Signed Add Entry 1997 Enhancements Prerequisite: signAdd97 .....	D-39
Table D-55: Signed Remove Entry 1997 Enhancements Prerequisite: signRemove97 .....	D-40
Table D-56: Signed Modify Entry 1997 Enhancements Prerequisite: signModify97.....	D-41
Table D-57: Signed Remove Entry 1997 Enhancements Prerequisite: signModDN97 .....	D-41
Table D-58: Signed Errors 1997 Enhancements Prerequisite: signErrors97.....	D-42
Table D-59: Security Parameters including 1997 Enhancements Prerequisite: .....	D-44
securityParams97	
Table D-60: 1997 Enhancements.....	D-45
Table D-61: 1997 Enhancements.....	D-46
Table D-62: Signed Errors 1997 Enhancements Prerequisite: signErrors97.....	D-47
Table D-63: 1997 Enhancements.....	D-47
Table D-64: Signed Shadow 1997 Enhancements Prerequisite: signShadRes97.....	D-48
Table D-65: Signed Errors 1997 Enhancements Prerequisite: signErrors97.....	D-48
Table D-66: Directory String Support .....	D-49

## SECTION I

### INTRODUCTION

#### 1. General

a. This annex profiles the X.500 directory to satisfy the functionality required in the Allied Directory. In general, responses to requirements for implementations are made in a PICS. In a few cases where tables do not exist in the PICS, responses are made in an ISP. Where PICS and ISPs do not exist (for the 1997 edition of the Directory, for example) PICS responses should be made in this profile.

b. Annex D is divided into four sections. Section II specifies additions to the requirements of the Directory ISPs. The ACP 133 profiles are defined by showing the differences and additions to the cited ISP tables. That is, the tables shown are adapted extracts (including notes) from the ISP tables. Text in the ISPs should be consulted for additional guidance.

c. For a particular ISP, the global table of conformance may show a predicate. For example, in Table D-1, item 9, the ACP 133 requires that a DSA be able to be used as a repository for strong authentication information. A predicate of `p_strong_rep` is set. In subsequent tables, support of attributes in the ISP that are conditional on `p_strong_rep` is mandatory.

d. Where parameters are mandated and default values are permitted, implementations shall also support non-default values.

e. Section III specifies system schema requirements for ADUAs based on the FDY12 ISP, which does not include DUA requirements because of the large variety of DUAs.

f. Section IV includes protocol and schema requirements beyond those in the current ISPs and PICS. A column, "PICS Response", is included in the tables in this section. These tables include items from X.402, RFC 1274, ACP 133-specified schema items, and selected items from the 1997 Directory standards. The completed tables should be submitted with the applicable PICS.

## SECTION II

### ACP 133 ADDITIONS TO CURRENT ISPS AND PICS

#### 2. Schema

##### a. Common Content

(1) DSAs and DUAs shall conform to ISO/IEC ISP 15126-1 (FDY11). The profile requirements for a single DSA for common directory use are given in Annex A and those for a

DUA in Annex B of that document. The additional requirements in the tables in this paragraph shall also be met. Column D represents the X.500 and X.400 standard requirement; column P represents the requirement of the ISP; column ACP represents the requirement of this profile. If the D & P requirements are the same, the columns are combined.

(2) Table D-1 is an adaptation of the table in clause A.1.2 in FDY11.

Table D-1  
Identification of the Implementation and/or System - Single DSA

Item	Question	D	P	ACP 133	Predicate
8	Can the DSA be configured as a first-level DSA	o	yes/ no	yes	p_firstlevel
9	Can the DSA be used as a repository for strong authentication information?	o	yes/ no	yes	p_strong_rep
12	Does the DSA support the Content Rule mechanism defined in ITU-T X.501   ISO/IEC 9594-2, 12.7?	o	yes/ no	yes	
13	Does the DSA support the Structure Rule mechanism defined in ITU-T X.501   ISO/IEC 9594-2, 12.6?	o	yes/ no	yes	
14	Does the DSA return Collective Attributes in respect to Read and Search operations?	o	yes/ no	yes	p_collective_Attr
15	Does the DSA fully support Collective Attributes in Search filter?	o	yes/ no	yes	p_collective_Attr
16	Does the DSA fully support Collective Attributes in Compare operations?	o	yes/ no	yes	p_collective_Attr
17	Does the DSA return Attribute Subtypes in respect to Read and Search operations?	o	yes/ no	yes	p_Attr_subtyping
18	Does the DSA fully support Attribute Subtypes in Search filter?	o	yes/ no	yes	p_Attr_subtyping
19	Does the DSA fully support Attribute Subtypes in Compare operations?	o	yes/ no	yes	p_Attr_subtyping

(3) Table D-2 is an adaptation of the table in clause B.1.2 in FDY11.

Table D-2  
Identification of the Implementation and/or System - DUA

Item	Question	D	P	ACP 133	Predicate
7	Does the DUA support strongAuthentication?	o	yes/ no	yes	p_strong
10	Does the DUA support Attribute Subtypes in respect to Read and Search operations?	o	yes/ no	yes	p_Attr_subtyping

(4) Table D-3 shows the collective attribute types, defined in X.520, that shall be supported. This is an adaptation of Table A.6.4.2.3 in FDY11.

Table D-3  
X.520 Collective Attribute Types

Ref. no.	Collective Attribute Type	D & P	ACP 133	Notes
1	collectiveLocalityName	o	m	
2	collectiveStateOrProvinceName	o	m	
3	collectiveStreetAddress	o	m	
4	collectiveOrganizationName	o	m	
5	collectiveOrganizationalUnitName	o	m	
6	collectivePostalAddress	o	m	
7	collectivePostalCode	o	m	
8	collectivePostOfficeBox	o	m	
9	collectivePhysicalDeliveryOfficeName	o	m	
10	collectiveTelephoneNumber	o	m	
11	collectiveTelexNumber	o	m	
12	collectiveTeletexTerminalIdentifier	o	m	

Table D-3  
X.520 Collective Attribute Types

Ref. no.	Collective Attribute Type	D & P	ACP 133	Notes
13	collectiveFacsimileTelephoneNumber	o	m	
14	collectiveInternationalISDNNumber	o	m	

(5) Table D-4 is an adaptation of the table in clause A.6.5.2 in FDY11.

Table D-4  
Standard Matching Rules

Ref. no.	Matching Rule	D	P	ACP 133	Notes
2	caseIgnoreOrderingMatch	o	o	m	
17	octetStringOrderingMatch	o	o	m	
25	uTCTimeOrderingMatch	o	o	m	
27	generalizedTimeOrderingMatch	o	o	m	
35	accessPointMatch	o	o	m	
36	masterAndShadowAccessPointMatch	o	o	m	
37	supplierAndConsumerMatch	o	o	m	
38	supplierOrConsumerInformationMatch	o	o	m	

b. Allied Directory System Schema

(1) DSAs and DUAs shall conform to ISO/IEC ISP 15126-2 (FDY12). The profile requirements for a single DSA are given in Annex A of that document. The additional requirements in the tables in this paragraph shall also be met. Column D represents the X.500 standard requirement; column P represents the requirement of the ISP; column ACP represents the requirement of this profile. If the D & P requirements are the same, the columns are combined.

(2) Table D-5 is an adaptation of the table in clause A.1.2 in FDY12.

Table D-5  
Identification of the Implementation and/or System - Single DSA

Item	Question	D	P	ACP 133	Predicate
7	Does the DSA support subschema administration?	o	yes/ no	yes	p_subschema
8	Does the DSA support collective attributes?	o	yes/ no	yes	p_collectiveAttr
9	Does the DSA support Simplified Access Control?	o	yes/ no	yes	p_AccessControl
10	Does the DSA support Basic Access Control?	o	yes/ no	yes	p_AccessControl
11	Does the DSA support Directory information shadow service specified in ITU-T X.525   ISO/IEC 9594?	o	yes/ no	yes	p_shadow

(3) Table D-6 is an adaptation of the table in clause A.6.4.2.1 in FDY12.

Table D-6  
Standard Operational Attribute Types - DSA Support

Ref. no.	Attribute Type	D & P	ACP 133	Notes
15	structuralObjectClass	o	m	
16	governingStructureRule	o	m	
22	myAccessPoint	o	m	
25	nonSpecificKnowledge	o	m	

### 3. DUAs

a. DUAs shall conform to ISO/IEC ISP 15125-1 (ADY11). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY11. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the Inter, Inter/Mod, and Adm columns represent the interrogation, interrogation/modification and administrative DUAs described in paragraph 219 of this ACP.

b. Table D-7 contains the differences from clause A.4.3.2.1, Operations.

Table D-7  
Operations

Item	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
3	Read	o	o	m	m	m	Read	
4	Compare	o	o	m	m	m	Compare	
5	Abandon	cn	c3	m	m	m	Abandon	Note 1
6	List	o	o	m	m	m	List	
7	Search	o	o	m	m	m	Search	
8	AddEntry	o	o	o	m	m	AddEntry	
9	RemoveEntry	o	o	o	m	m	RemoveEntry	
10	ModifyEntry	o	o	o	m	m	ModifyEntry	
11	ModifyDN	o	o	o	m	m	ModifyDN	

c3: If [Async-DUA], then support of this feature is o.

Note 1: The Abandon operation can only be supported if the asynchronous mode (ROSE class 2) of operation is supported for the DUA.

c. Table D-8 contains the differences from clause A.4.3.2.2, Extensions. This table defines a number of extensions which are available in the 1993 edition of the Directory. The supplier of the implementation shall indicate for which extensions conformance is claimed.

Table D-8  
Extensions

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
1	subentries	o	o	o	o	m		
4	extraAttributes	o	o	o	o	m		
5	modifyRightsRequest	o	o	o	o	m	modrightsreq	
10	useAliasOnUpdate	o	o	o	m	m		
11	newSuperior	o	o	o	o	m	newsuperior	

d. Table D-9 contains the differences from clause A.4.3.3.15, Service Controls.

Table D-9  
Service Controls

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
1	options	o	o	m	m	m		
2	priority	o	o	m	m	m		

e. Table D-10 contains the differences from clause A.4.3.3.16, Entry Information Selection.

Table D-10  
Entry Information Selection

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
3	extraAttributes	o	o	o	o	m		

f. DUAs shall conform to ISO/IEC ISP 15125-2 (ADY12). There are no additional requirements for ACP 133.

g. DUAs shall conform to ISO/IEC ISP 15125-5 (ADY41). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY41. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the Inter, Inter/Mod, and Adm columns represent the types of DUAs described in paragraph 219 of this ACP.

h. Table D-11 is an adaptation of the table in clause A.4.2.1 in ADY41.

Table D-11  
General Capabilities

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/Mod	Adm		
5	Does the DUA support signed DAP operations and results?	o	o	o	o	m	*digitalSig	

- i. Table D-12 is an adaptation of the table in clause A.4.2.2 in ADY41.

Table D-12  
Supported Security Levels

Item No.	Operation	D	P	ACP 133			Reference	Note
				Inter	Inter/Mod	Adm		
3	strong	cn	cl	m	m	m	*strongAuth	

cl: If [digitalSig], then support of this feature is m else o.

- j. Table D-13 is an adaptation of the table in clause A.4.3.1.1 in ADY41.

Table D-13  
Directory Bind Arguments

Item No.	Operation	D	P	ACP 133			Reference	Note
				Inter	Inter/Mod	Adm		
1.2.1	certification-path	c:o	c:o.1	m	m	m		
1.2.3	name	c:o	c:o.1	o	o	o		Note 1

- o.1 At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

Note 1: The name should be absent; the subject name within the user certificate contains the same information. Access control decisions should be based on authenticated information in the certificate, not on the unauthenticated name in the StrongCredentials.

- k. Table D-14 contains the differences from ADY41, clause A.4.3.3.22, Security Parameters. Requirements for use of the 1997 enhancements to security parameters for ACP 133 DUAs are specified in Annex D, Section IV, paragraph 7.

Table D-14  
Security Parameters

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/ Mod	Adm		
1	certification-path	m	m	c1	c1	m		Note 1
5	target	o	m	o	o	o		Note 2

c1: If [digitalSig], then support of this feature is m else o.

Note 1: As specified for the Certificate Management Infrastructure (CMI).

Note 2: The policy shall define minimum levels for the target protection levels.

1. Table D-15 is an adaptation of the table in clause B.3 in ADY41.

Table D-15  
General Security

Item No.	Operation	D	P	ACP 133			Predicate Name	Notes
				Inter	Inter/Mod	Adm		
2	Does the DUA support certificates?	o	o	m	m	m		
3	Does the DUA support Certificate Revocation List?	o	o	m	m	m		
4	Does the DUA support Authority Revocation List?	o	o	m	m	m	*arl	
5	Does the DUA support the ASN.1 Distinguished Encoding Rules (DER)?	o	o	m	m	m		Note 1

Note 1: DUAs shall conform to the encoding rules as specified in [ISO/IEC 9594-8: 1993 | ITU-T Rec. X.509 (1993)] Clause 9.

m. Table D-16 is an adaptation of the table in clause B.5 in ADY41.

Table D-16  
Strong Authentication

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/Mod	Adm		
1	Does the DUA support Strong Authentication on Bind Request?	o	o	m	m	m		Note 3
1.2	Two-way	c:o	c:o	m	m	m		

Table D-16  
Strong Authentication

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/Mod	Adm		
2	Does the DUA support Strong Authentication on Bind Result?	o	o	m	m	m		Note 3
3	Does the DUA support strong authentication in the initiator role?	o	o	m	m	m	*strong Auth	Note 3
4	Does the DUA support strong authentication in the responder role?	o	o	m	m	m	*strong Auth	Note 3
5	Does the DUA support the generation of certification path for strong authentication?	o	o	m	m	m	certPath	

Note 3: A positive response implies support for strong authentication (See A.4.2.2/3 in Annex A of ISP 15125-5)

n. Table D-17 is an adaptation of the table in clause B.6 in ADY41. Requirements for use of the 1997 signed operation enhancements for DAP in ACP 133 DUAs are specified in Section IV paragraph 7.

Table D-17  
Signed Operations

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/Mod	Adm		
5	Does the DUA support Signed Add Entry?	o	o	o	o	m	*signAdd	Note 5
6	Does the DUA support Signed Remove?	o	o	o	o	m	*signRemove	Note 5
7	Does the DUA support Signed Modify Entry?	o	o	o	o	m	*signModify	Note 5
8	Does the DUA support Signed ModifyDN?	o	o	o	o	m	*signModDN	Note 5

Note 5: A positive response implies support for Signed DAP operations (See A.4.2.1/5 in Annex A of ISP 15125-5)

#### 4. DSAs

##### a. DAP

(1) DSAs shall conform to ISO/IEC ISP 15125-3 (ADY21). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY21. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-18 contains the differences from clause A.4.2.1, General Capabilities.

Table D-18  
General Capabilities

Item No.	Operation	D	P	ACP	Predicate	Note
8	Is the DSA capable of supporting collective attributes?	o	o	m		
9	Is the DSA capable of supporting hierarchical attributes (Subtypes)?	o	o	m		

(3) Table D-19 contains the differences from clause A.4.3.2.1, Operations.

Table D-19  
Operations

Item No.	Operation	D	P	ACP	Predicate	Note
5	Abandon	cn	c3	m	*Abandon	

c3: If [Async-DSA], then support of this feature is o.

(4) DSAs shall conform to ISO/IEC ISP 15125-6 (ADY42). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY42. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(5) Table D-20 is an adaptation of the table in clause A.4.2.1 in ADY42.

Table D-20  
General Capabilities

Item No.	Operation	D	P	ACP	Reference	Notes
5	Does the DSA support signed DAP operations and results?	o	o	m	*digitalSig	

(6) Table D-21 is an adaptation of the table in clause A.4.2.2 in ADY42.

Table D-21  
Supported Security Levels

Item No.	Operation	D	P	ACP	Reference	Notes
3	strong	o.n	c1	m	*strongAuth	

c1: If [digitalSig ], then support of this feature is m else o.

(7) Table D-22 is an adaptation of the table in clause B.3 in ADY42.

Table D-22  
General Security

Item No.	Operation	D	P	ACP	Reference	Notes
2	Does the DSA support Certificates?	o	o	m		
3	Does the DSA support Certificate Revocation List?	o	o	m		
4	Does the DSA support Authority Revocation List?	o	o	m	*arl	
5	Does the DSA support the ASN.1 Distinguished Encoding Rules (DER)?	o	o	m		

(8) Table D-23 is an adaptation of the table in clause B.5 in ADY42.

Table D-23  
Strong Authentication

Item No.	Operation	D	P	ACP	Reference	Notes
1	Does the DSA support Strong Authentication on Bind Request?	o	o	m		
1.2	Two-way	c:o	c:o	m	*arl	
2	Does the DSA support Strong Authentication on Bind Result?	o	o	m		
3	Does the DSA support strong authentication in the initiator role?	o	o	m	*strongAuth	
4	Does the DSA support strong authentication in the responder role?	o	o	m	*strongAuth	
5	Does the DSA support the generation of certification path for strong authentication?	o	o	m		

(9) Table D-24 is an adaptation of the table in clause B.6 in ADY42. Requirements for use of the 1997 signed operation enhancements for DAP in ACP 133 DSAs are specified in Section IV, paragraph 8a.

Table D-24  
Signed Operations

Item No.	Operation	D	P	ACP	Reference	Notes
5	Does the DSA support Signed Add Entry?	o	o	m	*signAdd	
6	Does the DSA support Signed Remove Entry?	o	o	m	*signRemove	
7	Does the DSA support Signed Modify Entry?	o	o	m	*signModify	
8	Does the DSA support Signed ModifyDN?	o	o	m	*signModDN	

(10) DSAs shall conform to ISO/IEC ISP 15125-9 (ADY45). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY45. Column D represents the X.500 standards requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(11) Table D-25 shows the differences from clause A.4.2.3 of ADY45.

Table D-25  
Supported Access Control Schemes

Item No.	Question	D	P	ACP	Predicate	Note
2	Basic Access Control	o	o.1	m	*BAC-DSA	

(12) Table D-26 shows the differences from clause B.3 of ADY45.

Table D-26  
Access Support

Item No.	Question	D	P	ACP	Predicate	Note
7	Does the DSA support Import for entry access?	o	o	m	*importEntry	
8	Does the DSA support Export for entry access?	o	o	m	*exportEntry	
9	Does the DSA support ReturnDN for entry access?	o	o	m	*returnDNEntry	

b. DSP

(1) DSAs shall conform to ISO/IEC ISP 15125-4 (ADY22). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY22. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-27 shows the differences from clause A.3.1 of ADY22.

Table D-27  
DSA implementation and/or system

Item No.	Question	D	P	ACP	Predicate Name or note
6	Are Cross References supported?	o	o	m	p_cross_references
9	Are Master References supported	-	o	m	p_master_reference
12	Are Hierarchical operational bindings supported?	-	o	m	p_hob
18	Does the DSA support being a non-first-level DSA?	-	o	m	p_non_first_level_dsa
19	Does the DSA support the invoker role?	-	o	m	p_invoker
23	Does the DSA support strong credentials in the DSA Bind?	o	o	m	p_strong Note 2
24	Does the DSA support signed chained operations?	o	o	m	p_signed_chained Note 2
26	Does the DSA support authentication level? (see [ISO/IEC 9594-4: 1993   ITU-T Rec. X.518 (1993)] clause 10.3 m)	o	o	m	p_auth_level
28	Does the DSA support excludeShadows (see [ISO/IEC 9594-4: 1993   ITU-T Rec. X.518 (1993)] clause 10.3 q)	o	o	m	p_excludeShadows

Table D-27  
DSA implementation and/or system

Item No.	Question	D	P	ACP	Predicate Name or note
31	Does the DSA support creation of a request for cross-references (see [ISO/IEC 9594-4: 1993   ITU-T Rec. X.518 (1993)] clause 10.3 f)	o	o	m	p_obtain_xr
32	Does the DSA support the supply of cross-references on request (see [ISO/IEC 9594-4: 1993   ITU-T Rec. X.518 (1993)] clause 10.4 b)	o	o	m	p_supply_xr
33	Does the DSA support the request to return the operation to the DUA (see [ISO/IEC 9594-4: 1993   ITU-T Rec. X.518 (1993)] clause 10.10 i)	o	o	m	p_return_to_dua

Note 2: Security levels are profiled in ADY43. They are represented in this PRL by the predicates p\_simple\_protected (A.3.1.22), p\_strong (A.3.1.23), and p\_signed\_chained (A.3.1.24).

(3) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP. Requirements for use of the 1997 signed operation enhancements for DSP and DISP in ACP 133 are specified in Section IV, paragraphs 8b and 8c.

(4) Table D-28 specifies the differences from clause A.3.1, Global statement of conformance - DSP.

Table D-28  
Global Statement of Conformance - DSP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support DSA Binds in the initiator role?	o	o	m	p_dsa_bind_ini
2	Does the DSA support DSA Binds in the responder role?	o	o	m	p_dsa_bind_resp
5	Does the DSA support DSA Binds using strong credentials in the initiator role?	o	o	m	p_dsa_strong_ini
6	Does the DSA support DSA Binds using strong credentials in the responder role?	o	o	m	p_dsa_strong_resp
7	Does the DSA support the invoker role in DSP operations?	o	o	m	p_dsp_invoker
8	Does the DSA support signed DSP operations in both invoker and performer roles	o	o	m	p_signed_dsp
10	Does the DSA support authentication level in ChainingArguments	o	o	m	p_dsp_auth_level

(5) Table D-29 specifies the differences from clause A.3.4, Global statement of conformance - all supported protocols.

Table D-29  
Global Statement of Conformance - DSP, DOP, DISP

Item No.	Question	D	P	ACP	Predicate Name or note
2	Does the DSA support two-way authentication in strong binds?	o	o	m	p_2way_strong
3	Does the DSA support two-way authentication in signed operations?	o	o	m	p_2way_signed
8	Does the DSA support Certificate Revocation Lists Version 2?	o	o	m	p_crl_v2

(6) DSAs shall conform to ISO/IEC ISP 15125-13 (ADY61). Table D-30 specifies the differences from clause A.3.1, General Capabilities.

Table D-30  
General Capabilities

Item No.	Question	D	P	ACP	Predicate Name or note
2	Does the DSA support subschema administrative areas?	o	o	m	subschema
4	Does the DSA support access control inner administrative areas?	cl	cl	m	ACinner
5	Does the DSA support collective-attribute specific administrative areas?	o	o	m	ColAtSpec
6	Does the DSA support collective-attribute inner administrative areas?	o	o	m	ColAtInner
7	Does the DSA support multipurpose subentries?	o	o	m	MulPurSE

c.1: If BAC supported m then i.

(7) DSAs shall conform to ISO/IEC ISP 15125-9 (ADY45). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY45. Column D represents the X.500 standards requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(8) Table D-31 shows the differences from clause A.5.2.3 of ADY45.

Table D-31  
Supported Access Control Schemes

Item No.	Question	D	P	ACP	Predicate	Note
2	Basic Access Control	o	o.1	m	*BAC-DSA	

(9) Table D-32 shows the differences from clause B.3 of ADY45.

Table D-32  
Access Support

Item No.	Question	D	P	ACP	Predicate	Note
7	Does the DSA support Import for entry access?	o	o	m	*importEntry	
8	Does the DSA support Export for entry access?	o	o	m	*exportEntry	
9	Does the DSA support ReturnDN for entry access?	o	o	m	*returnDNEntry	

c. DISP

(1) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-33 specifies the differences from clause A.3.3, Global statement of conformance - DISP.

Table D-33  
Global Statement of Conformance - DISP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support the application-context: shadowSupplierInitiatedAC?	o	o	m	p_disp_sup_ini
2	Does the DSA support the application-context: reliableshadowSupplierInitiatedAC?	o	o	o	p_disp_rel_sup_ini Note 1
3	Does the DSA support the application-context: shadowConsumerInitiatedAC?	o	o	m	p_disp_cons_ini
4	Does the DSA support the application-context: reliableshadowConsumerInitiatedAC?	o	o	o	p_disp_rel_cons_ini Note 1
5	Does the DSA support DISP Binds in the initiator role?	o	o	m	p_disp_bind
6	Does the DSA support DISP Binds in the responder role?	o	o	m	p_disp_simp_unprot _resp

Table D-33  
Global Statement of Conformance - DISP

Item No.	Question	D	P	ACP	Predicate Name or note
9	Does the DSA support DISP Binds at least using strong credentials in the initiator role?	o	o	m	p_disp_strong_ini
10	Does the DSA support DISP Binds at least using strong credentials in the responder role?	o	o	m	p_disp_strong_resp
11	Does the DSA support signed DISP operations in both invoker and performer roles?	o	o	m	p_signed_disp

Note 1: The use of the RTSE-inclusive application contexts may be mandated by the tactical community.

(3) Table D-29 also applies.

(4) DSAs shall conform to ISO/IEC ISP 15125-10 (ADY51). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY51. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(5) Table D-34 specifies the differences from clause A.3 of ADY51.

Table D-34  
Global Statement of Conformance

Ref.No.	Question	D	P	ACP	Predicate	Notes
5	Is security level "strong" for peer entity authentication supported?	o.1	o	m	Strong-auth	
6	Are signed DISP operations supported?	o	o	m	Signed-ops	
7	Is the incremental update strategy supported?	o	o	m	Inc-updates	
8	Is secondary shadowing supported?	o	o	m		

o.1: At least one of the security levels for peer entity authentication shall be supported.

(6) DSAs shall conform to ISO/IEC ISP 15125-12 (ADY53). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to

ADY53. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(7) Table D-35 specifies the differences from clause A.3.1 of ADY53.

Table D-35  
DSA Implementation

Ref. No.	Question	Response	ACP
1	Shadow Supplier Role Supported	yes/no	yes
2	Shadow Consumer Role Supported	yes/no	yes
3	Empty Context Prefix in Replicated Area Supported	yes/no	yes

The following predicates are defined: p\_sup = A.3.1/1, p\_con = A.3.1/2, and p\_ecp = A.3.1/3

d. DOP

(1) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-36 specifies the differences from clause A.3.2, Global statement of conformance - DOP.

Table D-36  
Global Statement of Conformance - DOP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support Operational Binding type: shadowOperationalBindingID	o	o	m	p_sob
2	Does the DSA support Operational Binding type: SpecificHierarchicalBindingID	o	o	m	p_shob
4	Does the DSA support DOP Binds in the initiator role?	o	o	m	p_dop_bind_ini
5	Does the DSA support DOP Binds in the responder role?	o	o	m	p_dop_bind_resp

Table D-36  
Global Statement of Conformance - DOP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support Operational Binding type: shadowOperationalBindingID	o	o	m	p_sob
8	Does the DSA support DOP Binds using strong credentials in the initiator role?	o	o	m	p_dop_strong_ini
9	Does the DSA support DOP Binds using strong credentials in the responder role?	o	o	m	p_dop_strong_resp

(3) Table D-29 also applies.

(4) DSAs shall conform to ISO/IEC ISP 15125-16 (ADY71). The ACP requires support of both the shadowSupplierInitiatedAC and the ShadowConsumerInitiatedAC.

(5) DSAs shall conform to ISO/IEC ISP 15125-17 (ADY72). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY72. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(6) Table D-37 specifies the differences from clause 6 of ADY72.

Table D-37  
Summary of Support

Ref. No.	Question	P	ACP 133
10	Support of transfer of administrative point and subentry information by ROLE A DSAs: Subschema information	o	m
11	Support of transfer of administrative point and subentry information by ROLE A DSAs: Collective attribute information	o	m
18	Support of DOP binds using strong authentication	o	m

SECTION IIIDUA EXTENSIONS5. Administrative DUAs

a. Because of the variety of DUAs, FDY12 does not include any tables for DUAs. Table D-38 identifies support required for ACP 133 ADUAs, which are required to maintain operational attributes in the directory. Responses should be made in the PICS. Interrogation and Interrogation/Modification DUAs have no requirement to view or modify operational attributes.

Table D-38  
Identification of the Implementation and/or System - Administrative DUA

Item	Question	D	ACP 133	Predicate
1	Does the DUA support subschema administration?	o	yes	p_subschema
2	Does the DUA support collective attributes?	o	yes	p_collectiveAttr
3	Does the DUA support Simplified Access Control?	o	yes	p_AccessControl
4	Does the DUA support BasicAccess Control?	o	yes	p_AccessControl
5	Does the DUA support Directory information shadow service specified in ITU-T X.525   ISO/IEC 9594?	o	yes	p_shadow

b. Table D-39 shows the standard object classes that shall be supported by ADUAs.

Table D-39  
Standard Operational Object Classes - Administrative DUAs

Item	Object Class	D	ACP 133	Notes
1	subentry	m	C4	
2	subschemaSubentry	o	C1	

Table D-39  
Standard Operational Object Classes - Administrative DUAs

Item	Object Class	D	ACP 133	Notes
3	collectiveAttributeSubentry	o	C2	
4	accessControlSubentry	o	C3	

Conditionals:

C1: if p\_subschema then m else o.

C2: if p\_collectiveAttr then m else o.

C3: if p\_AccessControl then m else o.

C4: if p\_subschema or p\_collectiveAttr or p\_AccessControl then  
m else o.

c. Table D-40 shows the attribute types, defined in X.500 (1993), that shall be supported by ADUAs.

Table D-40  
Standard Operational Attribute Types - Administrative DUAs

Item	Attribute Type	D	ACP 133	Notes
1	createTimeStamp	m	m	
2	modifyTimeStamp	o	m	
3	creatorsName	o	m	
4	modifiersName	o	m	
5	administrativeRole	o	C4	
6	subtreeSpecification	o	m	
7	collectiveExclusions	o	C2	
8	dITStructureRules	o	C1	
9	dITContentRules	o	C1	
10	matchingRules	o	C1	
11	attributeTypes	o	C1	
12	objectClasses	o	C1	
13	nameForms	o	C1	
14	matchingRuleUse	o	C1	
15	structuralObjectClass	o	m	
16	governingStructureRule	o	m	
17	accessControlScheme	o	C3	
18	prescriptiveACI	o	C3	

Table D-40  
Standard Operational Attribute Types - Administrative DUAs

Item	Attribute Type	D	ACP 133	Notes
19	entryACI	o	C3	
20	subentryACI	o	C3	
21	dseType	o	m	
22	myAccessPoint	o	m	
23	superiorKnowledge	o	m	
24	specificKnowledge	o	m	
25	nonSpecificKnowledge	o	m	
26	supplierKnowledge	o	C5	
27	consumerKnowledge	o	C5	
28	secondaryShadows	o	C5	

Conditionals:

C1: if p\_subschema then m else o.

C2: if p\_collectiveAttr then m else o.

C3: if p\_AccessControl then m else o.

C4: if p\_subschema or p\_collectiveAttr or p\_accessControl then  
m else o.

C5: if p\_shadow then m else o.

#### SECTION IV

#### ACP 133 PROTOCOL AND SCHEMA EXTENSIONS

##### 6. Common Content Extensions

##### a. Object Classes

(1) Table D-41 shows the object classes, defined in X.402, that shall be supported.

Table D-41  
X.402 Object Classes

Item	Object Class	D	ACP 133	Notes	PICS Response
1	mhs-distribution-list	o	m		
2	mhs-message-store	o	m		
3	mhs-message-transfer-agent	o	m		
4	mhs-user	o	m		
5	mhs-user-agent	o	m		

(2) Table D-42 shows the object classes, defined in this ACP, that shall be supported.

Table D-42  
ACP 133 Object Classes

Item	Object Class	ACP 133	Notes	PICS Response
1	aCPNetworkEdB	m		
2	aCPNetworkInstructionsEdB	m		
3	addressList	m		
4	aliasCommonName	m		
5	aliasOrganizationalUnit	m		
6	altSpellingACP127	m		
7	cadACP127	m		
8	distributionCodeDescription	m		
9	distributionCodesHandled	m		
10	dSSCSPLA	m		
11	messagingGateway	m		
12	mLA	m	Note 1	
13	mLAgent	m		
14	network	m	Note 1	
15	networkInstructions	m	Note 1	
16	orgACP127	m		
17	otherContactInformation	m		
18	plaACP127	m		
19	plaCollectiveACP127	m		
20	plaData	m		
21	plaUser	m		

Table D-42  
ACP 133 Object Classes

Item	Object Class	ACP 133	Notes	PICS Response
22	releaseAuthorityPerson	m	Note 1	
23	releaseAuthorityPersonA	m		
24	routingIndicator	m		
25	securePkiUser	m		
26	secure-user	m	Note 1	
27	sigintPLA	m		
28	sIPLA	m		
29	spotPLA	m		
30	taskForceACP127	m		
31	tenantACP127	m		
32	ukms	m		

Note 1: These object classes may be removed in a later edition of this ACP.

(3) Table D-43 shows the object classes, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-43  
1997 Standard Object Classes

Item	Object Class	D	ACP	Notes	PICS Response
1	certificationAuthority-V2	o	m	Note 1	
2	cRLDistributionPoint	o	m		
3	userSecurityInformation	o	m		

Note 1: This object class may be removed in a later edition of this ACP.

(4) Table D-44 shows the object classes, defined in X.509(1997) DAM 1, that shall be supported.

Table D-44  
X.509(1997) DAM 1 Standard Object Classes

Item	Object Class	D	ACP	Notes	PICS Response
1	pkiCA	o	m		
2	pkiUser	o	m		

b. Attribute Types

(1) Table D-45 shows the attribute types, defined in X.402, that shall be supported.

Table D-45  
X.402 Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
1	mhs-acceptable-eits	o	m		
2	mhs-deliverable-classes	o	m		
3	mhs-deliverable-content-types	o	m		
4	mhs-dl-archive-service	o	m		
5	mhs-dl-members	o	m		
6	mhs-dl-policy	o	m		
7	mhs-dl-related-lists	o	m		
8	mhs-dl-submit-permissions	o	m		
9	mhs-dl-subscription-service	o	m		
10	mhs-exclusively-acceptable-eits	o	m		
11	mhs-maximum-content-length	o	m		
12	mhs-message-store-dn	o	m		
13	mhs-or-addresses	o	m		

Table D-45  
X.402 Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
14	mhs-or-addresses-with-capabilities	o	m		
15	mhs-supported-attributes	o	m		
16	mhs-supported-automatic-actions	o	m		
17	mhs-supported-content-types	o	m		
18	mhs-supported-matching-rules	o	m		
19	mhs-unacceptable-eits	o	m		

(2) Table D-46 shows the attribute types, defined in this ACP, that shall be supported.

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
1	accessCodes	m		
2	accessSchema	m	Note 1	
3	accountingCode	m		
4	aCPLegacyFormat	m		
5	aCPMobileTelephoneNumber	m		
6	aCPNetwAccessSchemaEdB	m		
7	aCPNetworkSchemaEdB	m		
8	aCPPagerTelephoneNumber	m		
9	aCPPreferredDelivery	m		
10	aCPTelephoneFacsimileNumber	m		

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
11	actionAddressees	m		
12	additionalAddressees	m		
13	additionalSecondPartyAddressees	m		
14	adminConversion	m		
15	administrator	m		
16	aigsExpanded	m		
17	aLExemptedAddressProcessor	m		
18	aliasPointer	m		
19	alid	m		
20	allowableOriginators	m		
21	aLReceiptPolicy	m		
22	alternateRecipient	m		
23	alType	m		
24	aprUKMs	m		
25	associatedAL	m		
26	associatedOrganization	m		
27	associatedPLA	m		
28	augUKMs	m		
29	cognizantAuthority	m		
30	community	m		
31	copyMember	m		
32	decUKMs	m		

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
33	deployed	m		
34	distributionCodeAction	m		
35	distributionCodeInfo	m		
36	dualRoute	m		
37	effectiveDate	m		
38	entryClassification	m		
39	expirationDate	m		
40	febUKMs	m		
41	garrison	m		
42	gatewayType	m		
43	ghpType	m		
44	guard	m		
45	hostOrgACP127	m		
46	infoAddressees	m		
47	janUKMs	m		
48	julUKMs	m		
49	junUKMs	m		
50	lastRecapDate	m		
51	listPointer	m		
52	lmf	m		
53	longTitle	m		
54	mailDomains	m		

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
55	marUKMs	m		
56	mayUKMs	m		
57	militaryFacsimileNumber	m		
58	militaryTelephoneNumber	m		
59	nameClassification	m		
60	nationality	m		
61	networkDN	m		
62	networkSchema	m	Note 1	
63	novUKMs	m		
64	octUKMs	m		
65	onSupported	m		
66	operationName	m		
67	plaAddressees	m		
68	plaNameACP127	m		
69	plaReplace	m		
70	positionNumber	m		
71	primarySpellingACP127	m		
72	proprietaryMailboxes	m		
73	publish	m		
74	rank	m		
75	recapDueDate	m		
76	releaseAuthorityName	m		

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
77	remarks	m		
78	rI	m		
79	rIClassification	m		
80	rIInfo	m		
81	secondPartyAddressees	m		
82	section	m		
83	secureFacsimileNumber	m		
84	secureTelephoneNumber	m		
85	sepUKMs	m		
86	serviceNumber	m		
87	serviceOrAgency	m		
88	sHD	m		
89	shortTitle	m		
90	sigad	m		
91	spot	m		
92	tARE	m		
93	tCC	m		
94	tCCG	m		
95	transferStation	m		

Table D-46  
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
96	tRC	m		
97	usdConversion	m		

Note 1: These attribute types may be removed in a later edition of this ACP.

(3) Table D-47 shows the attribute types, defined in RFC 1274, that shall be supported.

Table D-47  
RFC 1274 Attribute Types

Item	Attribute Type	ACP 133	Notes	PICS Response
1	host	m		
2	rfc822Mailbox	m	also known as mail	
3	roomNumber	m		

(4) Table D-48 shows the attribute types, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-48  
1997 Standard Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
1	attributeCertificate	o	m		
2	clearance	o	m	used in certificate extension	
3	deltaRevocationList	o	m		
4	supportedAlgorithms	o	m		

(5) Table D-49 shows the collective attribute types, defined in this ACP, that shall be supported.

Table D-49  
ACP 133 Collective Attribute Types

Item	Collective Attribute Type	D & P	ACP 133	Notes	PICS Response
1	collective-mhs-or-addresses	-	m		
2	collectiveMilitaryFacsimileNumber	-	m		
3	collectiveMilitaryTelephoneNumber	-	m		
4	collectiveNationality	-	m		
5	collectiveSecureFacsimileNumber	-	m		
6	collectiveSecureTelephoneNumber	-	m		

c. Name Forms

(1) Table D-50 shows the name forms, defined in this ACP, that shall be supported.

Table D-50  
ACP 133 Name Forms

Item	Name Form	D & P	ACP 133	Notes	PICS Response
1	aCPNetworkEdBNameForm	-	m		
2	aCPNetworkInstrEdBNameForm	-	m		
3	addressListNameForm	-	m		
4	aENameForm	-	m		
5	aliasCNNameForm	-	m		
6	aliasOUNameForm	-	m		
7	alternateSpellingPLANNameForm	-	m		
8	cadPLANNameForm	-	m		
9	distributionCodeDescriptionNameForm	-	m		
10	dSSCSPLANNameForm	-	m		
11	messagingGatewayNameForm	-	m		
12	mhs-dLNameForm	-	m		
13	mLANameForm	-	m	Note 1	
14	mLAgentNameForm		m		

Table D-50  
ACP 133 Name Forms

Item	Name Form	D & P	ACP 133	Notes	PICS Response
15	mSNameForm	-	m		
16	mTANameForm	-	m		
17	mUANameForm	-	m		
18	networkNameForm	-	m	Note 1	
19	networkInstructionsNameForm	-	m	Note 1	
20	organizationalPLANameForm	-	m		
21	organizationNameForm	-	m		
22	orgRNameForm	-	m		
23	orgUNameForm	-	m		
24	plaCollectiveNameForm	-	m		
25	qualifiedOrgPersonNameForm	-	m		
26	releaseAuthorityPersonNameForm	-	m	Note 1	
27	releaseAuthorityPersonANameForm		m		
28	routingIndicatorNameForm	-	m		
29	sigintPLANameForm	-	m		
30	sIPLANameForm	-	m		
31	spotPLANameForm	-	m		
32	taskForcePLANameForm	-	m		
33	tenantPLANameForm	-	m		

Note 1: These name forms may be removed in a later edition of this ACP.

b. Table D-51 shows the name forms, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-51  
1997 Standard Name Forms

Item	Name Form	D	ACP 133	Notes	PICS Response
1	cRLDistPtNameForm	o	m		

d. Matching Rules

Table D-52 shows the matching rules, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-52  
1997 Standard Matching Rules

Item	Matching Rule	D	ACP 133	Notes	PICS Response
1	algorithmIdentifierMatch	o	m		
2	attributeCertificateMatch	o	m	see Note	
3	attributeIntegrityMatch	o	o		
4	certificateExactMatch	o	o		
5	certificateListExactMatch	o	m		
6	certificateListMatch	o	m	see Note	
7	certificateMatch	o	m	see Note	
8	certificatePairExactMatch	o	o		
9	certificatePairMatch	o	m		
10	readerAndKeyIDMatch	o	m		*

\* Conditional on support of the encrypted variant of attributes as described in paragraph 408 of this ACP.

Note: Support for subelements of the matching rule is documented in the CMI CONOPS.

7. DUA Extensionsa. General

Table D-53 identifies use of the 1997 enhancements for security.

Table D-53  
1997 Security Enhancements

Item No.	Operation	D	ACP 133			Predicate Name	Note	PICS Response
			Inter	Inter/Mod	Adm			
1	Does the DUA support Signed Add Entry Enhancement?	o	o	o	m	signAdd97		
2	Does the DUA support Signed Remove Enhancement?	o	o	o	m	signRemove97		
3	Does the DUA support Signed Modify Entry Enhancement?	o	o	o	m	signModify97		
4	Does the DUA support Signed ModifyDN Enhancement?	o	o	o	m	signModDN97		
5	Does the DUA support Signed Errors	o	o	o	m	signErrors97		
6	Does the DUA support security parameters enhancement	o	o	o	m	securityParams97		

b. AddEntryResult

Table D-54 defines use of X.511 Signed Add Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.8, item 2.

Table D-54  
Signed Add Entry 1997 Enhancements  
Prerequisite: signAdd97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	AddEntryResult	m	m		
2.1	Null	c1	o		

Table D-54  
Signed Add Entry 1997 Enhancements  
Prerequisite: signAdd97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signAdd97] then support of this feature is m else "o".

c2 If [signAdd97] then support of this feature is m else "-".

c. RemoveEntryResult

Table D-55 defines use of X.511 Signed Remove Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.9, item 2.

Table D-55  
Signed Remove Entry 1997 Enhancements  
Prerequisite: signRemove97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	RemoveEntryResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signRemove97] then support of this feature is m else "o".

c2 If [signRemove97] then support of this feature is m else "-".

d. ModifyEntryResult

Table D-56 defines use of X.511 Signed Modify Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.10, item 2.

Table D-56  
Signed Modify Entry 1997 Enhancements  
Prerequisite: signModify97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	ModifyEntryResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signModify97] then support of this feature is m else "o"

c2 If [signModify97] then support of this feature is m else "-"

e. ModifyDNResult

Table D-57 defines use of X.511 Signed Modify DN 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.11, item 2.

Table D-57  
Signed Remove Entry 1997 Enhancements  
Prerequisite: signModDN97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	ModifyDNResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1: If Not [signModDN97] then support of this feature is m else "o".

c2: If [signModDN97] then support of this feature is m else "-".

f. Errors

Table D-58 defines use of X.511 Signed Errors 1997 Enhancements. Note: This updates Clause A.4.3.3.12 in ADY11 for signed errors and replaces A.4.3.3.12 in ADY41. Support for problem codes shall be as in ADY11 and ADY41. The following uses predicates defined in ADY11.

Table D-58  
Signed Errors 1997 Enhancements  
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
1	Abandoned	cn	c10		
1.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
1.1	CommonResults	c:m	m		
1.1.1	Security Parameters	c:m	m	see Table D-59	
1.2	algorithmIdentifier	c:m	m		
1.3	encrypted	c:m	m		
2	AbandonFailed	cn	c10		
2.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
2.1	problem	c:m	c:m	As in ADY11	
2.2	operation	c:m	c:m	As in ADY11	
2.3	CommonResults	c:m	m		
2.4.1	Security Parameters	c:m	m	see Table D-59	
2.5	algorithmIdentifier	c:m	m		
2.6	encrypted	c:m	m		
3	AttributeError	cn	c11		
3.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
3.1	object	c:m	c:m	As in ADY11	
3.2	problems	c:m	c:m	As in ADY11	
3.2.1	problem	c:m	c:m	As in ADY11	
3.3	type	c:m	c:m	As in ADY11	
3.4	value	c:o	c:m	As in ADY11	
3.5	CommonResults	c:m	m		
3.5.1	Security Parameters	c:m	m	see Table D-59	
3.6	algorithmIdentifier	c:m	m		
3.7	encrypted	c:m	m		
4	NameError	cn	c12		
4.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	

Table D-58  
Signed Errors 1997 Enhancements  
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
4.1	problem	c:m	c:m	As in ADY11	
4.2	matched	c:m	c:m	As in ADY11	
4.3	CommonResults	c:m	m		
4.3.1	Security Parameters	c:m	m	see Table D-59	
4.4	algorithmIdentifier	c:m	m		
4.5	encrypted	c:m	m		
5	Referral	cn	i	See ADY12	
5.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
5.1	candidate	c:m	-	See ADY12	
5.2	CommonResults	c:m	m		
5.2.1	Security Parameters	c:m	m	see Table D-59	
5.3	algorithmIdentifier	c:m	m		
5.4	encrypted	c:m	m		
6	SecurityError	cn	c12		
6.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
6.1	problem	c:m	c:m	As in ADY11	
6.2	CommonResults	c:m	m		
6.2.1	Security Parameters	c:m	m	see Table D-59	
6.3	algorithmIdentifier	c:m	m		
6.4	encrypted	c:m	m		
7	ServiceError	cn	c12		
7.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
7.1	problem	c:m	c:m	As in ADY11	
7.2	CommonResults	c:m	m		
7.2.1	Security Parameters	c:m	m	see Table D-59	
7.3	algorithmIdentifier	c:m	m		
7.4	encrypted	c:m	m		
8	UpdateError	cn	c14		
8.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
8.1	problem	c:m	c:m	As in ADY11	
8.2	CommonResults	c:m	m		
8.2.1	Security Parameters	c:m	m	see Table D-59	

Table D-58  
Signed Errors 1997 Enhancements  
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
8.3	algorithmIdentifier	c:m	m		
8.4	encrypted	c:m	m		

- c10: If [Abandon], then support of this feature is m else o.  
c11: If [Read or Compare or Search or AddEntry or ModifyEntry], then support of this feature is m else o.  
c12: If [Read or Compare or List or Search or AddEntry or RemoveEntry or ModifyEntry or ModifyDN], then support of this feature is m else o.  
c13: If [pageresreq], then support of this feature is m else -.  
c14: If [AddEntry or RemoveEntry or ModifyEntry or ModifyDN], then support of this feature is m else o.

g. Security Parameters

Table D-59 defines use of X.511 1997 Security Parameters. Note: This replaces clause A.4.3.3.22 in ADY 41.

Table D-59  
Security Parameters including 1997 Enhancements  
Prerequisite: securityParams97

Item No.	Protocol Element	D	P	ACP 133	Note	PICS Response
1	certification-path	m	m	m	see Note 1	
2	name	o	m	m		
3	time	o	m	m	see Note 2	
4	random	o	m	m	see Note 2	
5	target	o	m	o	see Note 3	
6	response	o	i	o		
7	operationCode	o	i	m	see Notes 4 & 5	
8	attribute CertificationPath	o	i	o		
9	errorProtection	o	i	o	see Note 3	
10	errorCode	o	i	m	see Notes 6 & 7	

Note 1: As specified for the Certificate Management Infrastructure (CMI).

Note 2: In request set as specified in X.511 '93 (need not be related in sequence to previous operations). In results or error this shall be set by the DSA and checked by the DUA to be the value of random in request argument plus 1 as specified in X.511 1997.

The receiving DSA shall use time and “random” to ensure that an earlier request is not replayed.

Note 3: The policy shall define minimum levels for the target and error protection levels.

Note 4: This shall be the same as the code for the operation being carried out.

Note 5: A defect has been raised on the syntax for operationCode.

Note 6: This shall only be present if an error is being returned and shall be the same as the returned error code.

Note 7: A defect has been raised adding this errorCode to Security Parameters.

## 8. DSA Extensions

### a. DAP

(1) Table D-60 identifies use of the 1997 enhancements for security.

Table D-60  
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed Add Entry Enhancement?	o	m	signAdd97		
2	Does the DSA support Signed Remove Enhancement?	o	m	signRemove97		
3	Does the DSA support Signed Modify Entry Enhancement?	o	m	signModify97		
4	Does the DSA support Signed ModifyDN Enhancement?	o	m	signModDN97		
5	Does the DSA support Signed Errors		m	signErrors97		
6	Does the DSA support security parameters enhancement		m	securityParams97		

(2) The support for signed AddEntryResult shall be as defined in Table D-54. Note: This replaces ADY 42 A.4.3.3.8 item 2.

(3) The support for signed RemoveEntryResult shall be as defined in Table D-55. Note: This replaces ADY 42 A.4.3.3.9 item 2.

(4) The support for signed ModifyEntryResult shall be as defined in Table D-56. Note: This replaces ADY 42 A.4.3.3.10 item 2.

(5) The support for signed ModifyDNResult shall be as defined in Table D-57. Note: This replaces ADY 42 A.4.3.3.10 item 2.

(6) The support for signed Errors shall be as defined in Table D-58. Note: This updates ADY21 Clause A.4.3.3.12 and ADY 42 A.4.3.3.12. Support for problem codes shall be as in ADY21 and ADY42.

(7) The support of the security parameters field shall be as defined in Table D-59. Note: This replaces clause A.4.3.3.22 in ADY 42.

b. DSP

(1) Table D-61 identifies use of the 1997 enhancements for security.

Table D-61  
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed Errors	o	m	signErrors97		

(2) The support for signed errors shall be as defined in Table D-58 with the exception that item 5 (Referral) is replaced with DSAReferral in Table D-62. Note: This replaces Clause A.4.3.5 in ADY22 for signed errors.

Table D-62  
Signed Errors 1997 Enhancements  
Prerequisite: signErrors97

Deleted: D-

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
5	DSAReferral	cn	i	See ADY12	
5.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
5.1	continuationPrefix			See ADY12	
5.2	contextPrefix	c:m	-	See ADY12	
5.3	CommonResults	c:m	m		
5.3.1	Security Parameters	c:m	m	see Table D-59	
5.4	algorithmIdentifier	c:m	m		
5.5	encrypted	c:m	m		

(3) The support of the security parameters field shall be as defined in Table D-59.

Note: This replaces clause A.7.2 in ADY 43.

c. DISP

(1) Table D-63 identifies use of the 1997 enhancements for security.

Table D-63  
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed shadow result Enhancement?	o	m	signShadRes97		
2	Does the DSA support Signed Errors		m	signErrors97		
3	Does the DSA support security parameters enhancement		m	securityParams97		

(2) Table D-64 defines use of Signed Shadow 1997 enhancement. Note: This replaces ADY43, A.6.1.2.3, item 12.

Table D-64  
Signed Shadow 1997 Enhancements  
Prerequisite: signShadRes97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
12	xxx-result	m	m		
12.1	Null	c1	o		
12.2	information	c2	m		
12.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
12.2.2	CommonResults	c2	m		
12.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signShadRes97], then support of this feature is m else "o".

c2 If [signShadRes97], then support of this feature is m else "-".

(3) Table D-65 defines use of X.525 Signed Errors 1997 Enhancements. Note: This replaces ADY51, A.4.3.6 for signed errors.

Table D-65  
Signed Errors 1997 Enhancements  
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
1	shadowError	m	m	As in ADY51	
2	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
3	problem		m	As in ADY51	
4	lastUpdate	o	m	As in ADY51	
5	updateWindow	o	m	As in ADY51	
3	CommonResults	c:m	m		
4	Security Parameters	c:m	m	see Table D-59	
5	algorithmIdentifier	c:m	m		
6	encrypted	c:m	m		

(4) The support of the security parameters field shall be as defined in Table D-59. Note: This replaces use of security parameters in ADY 51, clauses A.4.3.3, A.4.3.4 and A.4.3.5.

9. Schema Extensions

Table D-66 summarizes the requirement to support the Universal Character String Transformation Format 8 (UTF-8) encoding of the ISO/IEC 10646 Character Set. This string type will be usable wherever the Directory String type is used, e.g., Distinguished name, public key certificates. (PrintableString and TeletexString are required to be supported by the X.500 standard.) A proposed amendment to X.519 and X.520 to add a choice of UTF-8 to the definition of DirectoryString is expected to be approved in 1999.

Table D-66  
Directory String Support

Item	Matching Rule	D	ACP 133	Notes	PICS Response
1	Does the DSA Support UTF-8 strings?	o	m		

10. Corrigenda not included in ISPs

[Ed.: To be supplied.]

APPENDIX 1 TO ANNEX D

DEFECT REPORT FORM

1. Defect Report Number:  
Title: Use of Operation and Error Code in Security Parameters
2. Source:
3. Addressed to:
  - (a)
  - (b)
4. Date circulated by WG Secretariat:
5. Deadline for Response from Editor:
6. Defect Report Concerning:  
ITU-T X.511 (1997) | ISO/IEC 9594-3:1997
7. Qualifier:  
Error and Omission
8. References in Document:  
Clause 7.10
9. Nature of Defect:
  - (a) The syntax of operationCode in Security Parameters is currently defined as an Object Identifier. However, Remote Operation Service (ROS) Operation Codes may be either Integer or Object Identifier and currently all the X.500 operation codes are defined as Integers.
  - (b) Since error codes are not protected a similar attack can occur on error responses to the attack on operation codes. Where both a successful response and error contains signed Security Parameters with no extra parameters (e.g. Modify Response and Abandon Error), the unprotected part of a PDU may be altered to change an error to success without detection.

10. Solution Proposed by the Source:

In clause 7.10:

- (a) Replace syntax for operationCode in SecurityParameters to be:

operationCode [6] Code OPTIONAL

Code should be imported from:

Remote-Operations-Information-Objects {  
joint-iso-ccitt remote-operations(4) informationObjects(5) version1(0) }

and in the paragraph describing **operationCode** delete “object identifier”. Also, at end of paragraph change “or results” to “, results or errors”.

- b) Add to the SecurityParameters syntax:

errorCode [9] Code OPTIONAL

and add the following description:

The **errorCode** is used to secure the error code where an error is returned in response to an operation.

11. Editor’s Response:

ANNEX EEXAMPLE SHADOWING AGREEMENT

Table E-1	
Example Shadowing Agreement Checklist	
Legend:	
SD	indicates the shadow Supplier DSA administrator must provide information/initial agreement
CD	indicates the shadow Consumer DSA administrator must provide information/initial agreement
MD	indicates the Master DSA administrator must initial agreement
DM	indicates the Directory Services Manager must initial agreement
<b>Supplier DSA (SD)</b>	
DSA Name:	
DSA location (including building & room number):	
Communications address:	
Primary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	
Postal address:	
Secondary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	
Postal address:	
Tertiary Point of Contact (24 hours, 7 days a week):	
Commercial telephone number:	
Military telephone number:	
<b>Consumer DSA (CD)</b>	
DSA Name:	
DSA location (including building & room number):	
Communications address:	
Primary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	
Postal address:	
Secondary Point of Contact name:	
Commercial telephone number:	

Table E-1	
Example Shadowing Agreement Checklist	
Military telephone number:	
E-mail address:	
Postal address:	
Tertiary Point of Contact (24 hours, 7 days a week):	
Commercial telephone number:	
Military telephone number:	
<b>Agreements</b>	
1.(SD)___ (CD)___ Both DSAs involved in this agreement are ACP 133 compliant DSAs.	
2.(SD)___ (CD)___ Both DSAs involved in this agreement operate under compatible security policies.	
3. If the consumer DSA is to act as a backup to the supplier DSA, this section must be completed.	
(CD)___ The consumer DSA understands and agrees that if the supplier DSA fails or is unavailable, that the consumer DSA must support the supplier DSA agent's accesses.	
(SD)___ During a normal 8-hour working period the supplier DSA unit of replication is accessed approximately _____ times. During the worst case 8-hour period the unit of replication has or may experience approximately _____ accesses.	
4. X.500 standard shadowing specifications	
(SD)_____ (CD)_____ The Unit of Replication is:	
Area Specification:	
Context Prefix: _____	
Subtree Specification:	
Base: _____	
Chop: _____	
Filter (object classes): _____	
Attribute Selection:	
All attributes _____ or	
Include attributes: _____	
_____	
Exclude attributes: _____	
_____	
Include knowledge held of _____ master and/or _____ shadow naming contexts.	
Update Mode: _____	
Master: _____	
Secondary Shadows: _____	
_____	

Table E-1 Example Shadowing Agreement Checklist	
5.(SD)_____	The supplier DSA information area to be replicated contains _____ kbytes (includes a 30% growth factor). If the replicated area grows beyond this size, the supplier DSA agrees to immediately re-negotiate to amend this agreement.
(CD)_____	The consumer DSA acknowledges the size of the shadow copy to be held.
6.(SD)_____	During a normal 8-hour working period the supplier DSA unit of replication is modified (entries added, deleted, changed) approximately _____ times.
(CD)_____	The consumer DSA acknowledges the impact of the modifications.
7.(SD)_____	The supplier DSA was, in the last 90 days if possible, on-line and accessible _____% of the time.
(CD)_____	The consumer DSA was, in the last 90 days if possible, on-line and accessible _____% of the time.
(SD)_____ (CD)_____	The supplier DSA and consumer DSA acknowledge the reliability rate.
8.(SD)_____ (CD)_____	The supplier and consumer DSAs agree to immediately notify each other in the event either DSA fails or is otherwise unavailable for service.
9.(SD)_____ (CD)_____	The supplier and consumer DSAs (points of contact) agree this shadowing agreement shall go into effect at _____ UTC and remain in effect until _____ UTC.
10.(SD)_____ (CD)_____	This agreement may be terminated by either the consumer or supplier DSAs if terms and conditions in this agreement are modified without re-negotiation.
11.(CD)_____	The consumer DSA agrees to provide 30 days notification, if for any reason the consumer DSA will be unable to fulfill this agreement.
(SD) _____	The supplier DSA agrees to provide 30 days notification, if for any reason the supplier DSA will be unable to fulfill this agreement.

Table E-1 Example Shadowing Agreement Checklist	
12.(CD)_____	Further constraints/conditions of the supplier DSA: _____ _____ _____
(SD)_____	Further constraints/conditions of the consumer DSA: _____ _____ _____
13.(SD)_____ (CD)_____ If update is to occur upon changes, the maximum period over which changes are accumulated before the shadowing is done is _____.	
14.(DM)_____ The Directory Services Manager agrees that this agreement is consistent with policy and that the topology involved is consistent with replication policy regarding the best choice for minimizing hops and single point of failure avoidance.	
15.(MD)_____ If this agreement is for secondary shadowing, the Master DSA administrator agrees that the agreement is consistent with the information owner's policy.	
16. Protection provided to shadowed information Type of Authentication None_____ Simple_____ Strong_____ Variable (as per ACI shadowed) _____ Type of Access Control Basic_____ Simplified_____ Rule-Based_____ General Protection (for read access); restricted to these users: _____  (CD)_____The consumer will apply ACI that is shadowed with the unit of replication.	
17. When a shadowing agreement is terminated, the shadow consumer agrees to remove the shadowed information from the consumer DSA within time period_____.	
18. Auditing that will be done by the consumer on shadowed information and details on access to and archive of audit data.	

Note that indicating that secondary shadowing of the subject information can be performed does not preclude the

necessity for each secondary shadow being (part of) the subject of a (secondary) shadowing agreement.



ANNEX F

EXAMPLE SERVICE LEVEL AGREEMENT

**SERVICE LEVEL AGREEMENT**  
**BETWEEN THE**  
**< NAMES OF ORGANIZATIONS >**  
**FOR THE**  
**PROVISION OF DIRECTORY SERVICES**

VERSION HISTORY

	<b>Section</b>	<b>Issue</b>	<b>Date of Issue</b>	<b>Remarks</b>
Main Document	Service Level Agreement			
Appendix A	Service Profiles			
Appendix B	Management and Reporting Criteria			
Appendix C	Management Points of Contact			
Appendix D	Finance			

DISTRIBUTION

<b>COPY NUMBER</b>	<b>HOLDER</b>	<b>LOCATION</b>
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

CONTENTS

DEFINITIONS

- Services** The provision of planning, procurement, implementation, change control, task coordination, project management, configuration management, maintenance, security, documentation, operator services, quality control, and financial management of <assets> within the <organization> area of responsibility.
- Customer** The organization receiving directory services from the <service provider>. The Customer will be represented by a nominated person for each Customer site representing all users of services.
- SLA Review Meeting** The SLA Review Meeting is held to discuss and approve any changes required to the SLA document. Chaired by <as appropriate>.
- Project Review Board** The Project Review Board (PRB) meets to discuss policy and strategic level project issues. It is chaired by <as appropriate>.

GLOSSARY

1. ACP Allied Communication Publication

REFERENCES

1. ACP 133 version < >

## INTRODUCTION

### PURPOSE OF THIS DOCUMENT

1. This section gives details of the participating governments. It gives any background to the requirement for the establishment of electronic directory services. It mentions that the SLA exists for the further cooperation relating to the relating to the establishment, assignment, utilization, practices and payment for electronic directory services shared or provided between the participating organizations.

### SCOPE

2. The scope covers the provision of electronic directory services by giving a brief, high level description of the services being provided, information regarding the provision of resources and any relevant instructions and constraints. Also covered is amendment or cancellation and its effect on the SLA.

### RESPONSIBILITIES

3. Identifies those parties/authorities responsible for the implementation of the agreement. It details the levels at which coordination between the parties can take place. The specific technical details for the levels of service, procedures and practices, restoration, leasing and postal and communications addresses and funding are to be included in Appendices referenced from this section.

### IMPLEMENTATION

4. Each party will have responsibility for its own directory systems, including the procurement and maintenance of equipment and services. Working level details will need to be outlined within appendices to the document and should include, where necessary, details of the responsibilities and tasks one nation may offer another nation in setting up the service. It should designate any project planning time scales.

### SERVICES TO BE PROVIDED

5. Service Profiles - The Provider will meet the Customer-specific requirements detailed in Appendix A to this SLA.

6. Management and Reporting Criteria - The Provider will deal with fault conditions in accordance with Appendix B.

7. Management Points of Contact - Points of contact at various levels in the management chain are given in Appendix C.

#### FUNDING

8. This section makes statements about who has financial responsibility for different parts of the system. As in establishing a bilateral agreement between two nations, both nations will benefit from a mutual exchange of information which may imply that there would be no costs levied for the provision of the service. Each party would normally bear the costs of its own operations and maintenance. Also included would be any reimbursements of costs. An appendix giving the precise details of costs would be referenced.

#### SECURITY

9. Details are to be given of the classification of the directory service and the security mechanisms to be implemented.

#### RELEASE OF INFORMATION

10. The rules of release of one nation's information to others, including members of its own Armed Forces, public and press. The mechanisms to undertake the safeguarding of protectively marked material as well as the handling of unclassified material.

#### WAIVER OF CLAIMS

11. Statements on waiver of claims resulting from loss, damage or failure of equipment.

#### ARBITRATION AND DISPUTES

12. A statement constraining the parties to resolve any disagreements between themselves and limiting the level of escalation.

#### ENTRY INTO FORCE, TERMINATION, AND REVIEW

13. Statements covering the bringing into force of the agreement, its length of validity, notice of termination and the period of review for the agreement are to be given, including any requirement for review meetings.

**AUTHORITY FOR AGREEMENT**

Signed for and on behalf of <responsible initiating authority>

Date: \_\_\_\_\_ Signature: \_\_\_\_\_

<Rank/Name/Position>

Signed for and on behalf of the <other party>

Date: \_\_\_\_\_ Signature: \_\_\_\_\_

<Rank/Name/Position>

**APPENDIX A - SERVICE PROFILES**

1. The tables below define the service profiles available for each of the provided services.

**DIRECTORY SERVICE (for example)**

<b>SERVICE ATTRIBUTES</b>	<b>SERVICE OPTION No.</b>	<b>SERVICE OPTION DESCRIPTION</b>
<b>FEATURES</b>	1a	
	1b	
<b>SECURITY</b>	2a	UNCLASSIFIED
	2b	RESTRICTED
	2c	SECRET
<b>MANAGEMENT</b>	3a	No Control or Monitoring
	3b	Central Control and Monitoring
	3c	
	3d	Local control only
<b>SURVIVABILITY</b>	4a	Standard
	4b	Physical security
	4c	Blast protected
	4d	EMP protected
	4e	Route Diversity
<b>INTERFACES</b>	6a	
	6b	
<b>PERFORMANCE</b>	7	
<b>PERFORMANCE (Site Service Availability measured over 1 year)</b>	7a	x%
	7b	x%
<b>PERFORMANCE (Grade of Service)</b>	7d	
<b>SYNCHRONIZATION</b>		
<b>MAINTENANCE</b>	9a	Next working day attention
	9b	4 hour maximum time to respond 0800-1700 Mon to Fri
	9c	4 hour maximum time to respond at any time
	9d	4 hour mean time to repair at any time

### CONFIGURATION DETAILS

2. This section shall include directory configuration details covering:
  - Naming Context
  - Knowledge information
  - Shadowing agreements
  - Secondary Shadowing authorizations
  - Underlying protocol stack
  - Replication agreements
3. Protocol Profiles are required for DAP, DISP, DOP, and DSP.

### ACCESS CONTROL PROFILES

4. Any national directory system contains national preferences for Access Control. An agreed Access Control Infrastructure will need to be developed and the profiles recorded.
5. A key and certificate management regime will be required if the directory system may require its interfaces (DAP, DSP, DISP and DOP, if used), to be fully authenticated.

### ADMINISTRATIVE PROFILES

6. Profiles are required for ADUAs.
7. An agreement will need to be made on clock synchronization.

### APPENDIX B - MANAGEMENT AND REPORTING CRITERIA

1. This appendix details the Customer-specific requirements of service management and reporting.

### FAULT REPORTING AND HELP SERVICES

2. When a fault condition occurs, the Customer is first to check that it has not been caused by the Customer's equipment. Once satisfied that this is not the case, the Customer will submit a fault report to the service provider.
3. A Help desk will be established to provide the first point of customer contact for service queries and will be able to answer both technical and procedural questions.

## SERVICE RESTORATION

4. Following a fault, the Provider will ensure that the service is restored within the <defined> time scales. A service will not be considered to be restored until positive confirmation has been obtained from the Customer. During service restoration the Provider will provide the Customer reporting the fault with progress information.
5. The specified restoration time is to start from the receipt of the fault report by the help desk, unless the fault is initially detected by the Provider, in which case the restoration time is to start from the time of detection.
6. The Provider will provide the Customer reporting the fault with the following information during fault restoration:
  - Within 30 minutes of the report of a fault, provide an estimate of the restoration time.
  - If it becomes apparent that the estimated restoration time will not be met, immediately advise the Customer accordingly, and as soon as possible thereafter advise the Customer of the new forecast restoration time.
7. If the Provider fails to meet the restoration time for a service, as specified in Appendix A, he is to take the following actions:
  - Inform the Customer immediately, agree the update rate with the Customer, and provide a new estimated restoration time.
  - Formally record the failure to meet the restoration time, and provide a written report to the Customer.
  - The Help Desk will, on request from a Customer, provide details of contacts through whom the requirement for fault restoration can be escalated.

## REAL TIME MONITORING

8. The Provider will monitor and analyze performance criteria in real time to identify shortfalls against Appendix A and manage the system proactively by:
  - Informing the Customer of faults that Customers may not be aware of but which may affect Customer services.
  - Offering advice on alternative services under fault conditions.

INVESTIGATIONS AND REPORTING

9. The Provider will provide the Customer with the following routine reports:

- A monthly summary of actual performance against the requirements contained within this agreement and actions in hand to correct any deficiencies.
- A quarterly report covering technical, operational <and financial performance>.
- An annual report covering audits and any service development plans produced by the contractors.

10. The Provider will undertake investigations and provide the Customer with special reports, on request, under the following circumstances:

- Persistent failure to meet one or more performance targets.
- Major loss of service or catastrophic failure.

SCHEDULED LOSS OF SERVICE

11. The Provider will give the Customer one calendar month written notice of any proposed scheduled loss of service. Any variation from this is to be agreed on an exceptional basis only. The timing, extent and duration of any such loss of service is to be negotiated and agreed by the Provider and the Customer on a case by case basis.

SERVICE PROVISION

12. The Provider will supply a service in the planning and implementation of minor and major projects. The Provider is to meet, from receipt of the requirement, the specified time scales for the three categories as shown below:

Category	Time scale
Operational	<Two days> Earlier time scale, if achievable, to be agreed within 24 hours of receipt
Priority	<Five days> Earlier time scale, if achievable, to be agreed within 24 hours of receipt
Normal (baseline)	

13. Moves and changes will be delivered as follows:

- 85 % of scheduled site housekeeping routines completed within one day of agreed scheduled time.
- 85 % of system software controlled moves and changes completed within one working day.
- <> % of on site small physical moves and changes completed within <> working days of receipt of request.

**DOCUMENTATION**

14. The Provider will issue to the Customer sufficient copies of documents to allow efficient use of the services provided.

**MEETINGS**

15. <As Appropriate>

**APPENDIX C - MANAGEMENT POINTS OF CONTACT**

The tables below show the normal levels at which contact is made:

**Hour by Hour Management**

<b>Service Provider</b>	<b>Customer</b>
<b>Help Desks:</b>	
<b>System Supervisor:</b>	

Policy and Management Escalation

Service Provider	Customer
Action Office:	

**APPENDIX D - FINANCE**

1. This appendix should contain details of the financial arrangements between the parties, including costs incurred and any accrued credits or liabilities.
2. Each party would normally bear the costs of operation and maintenance of its own directory infrastructure.

ANNEX G  
ABBREVIATIONS

The following abbreviations and acronyms are used in this ACP:

ACDF	Access Control Decision Function
ACI	Access Control Information
ACP	Allied Communication Publication
ACSE	Association Control Service Element
ADUA	Administrative Directory User Agent
ADY	1993 Directory Application Profile
AIG	Address Indicator Group
AL	Address List
AMH	Allied Message Handling
APP	Allied Publications Procedures
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
AU	Australia
AUTODIN	Automatic Digital Network
BAC	Basic Access Control
C	Country
CA	Canada; Certification Authority
CAD	Collective Address Designator
CCEB	Combined Communications Electronics Board
CCITT	The International Telegraph and Telephone Consultative Committee
CMI	Certificate Management Infrastructure

CMIP	Common Management Information Protocol
CN	Common Name
CONOPS	Concept of Operations
COSINE	Organization for Cooperation for OSI Networking in Europe
COTS	Commercial Off-the-Shelf
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSP	Common Security Protocol
CTF	Combined Task Force
CULR	Common Upper Layer Requirements
DAG	DSSCS Address Group
DAP	Directory Access Protocol
DFTS	Defense Fixed Telecommunications Service
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DL	Distribution List
DMD	Directory Management Domain
DN	Distinguished Name
DODAAC	Department of Defense Activity Accounting Code
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSE	DSA-specific entry
DSN	Defense Switched Network
DSP	Directory System Protocol

DSSCS	Defense Special Security Communications System
DUA	Directory User Agent
EDI	Electronic Data Interchange
EIT	Encoded Information Type
E-MAIL	Electronic Mail
EOS	Elements of Service
FDY	1993 Directory Interchange Format and Representation Profile
FLDSA	First-level DSA
G3	Group 3 Facsimile
G4	Group 4 Facsimile
GENSER	General Service
GHP	Gateway Handling Policy
HOB	Hierarchical Operational Binding
HQ	Headquarters
IA5	International Alphabet Number 5
IBAC	Identity-based Access Control
IC	Intelligence Community
IEC	International Electrotechnical Commission
ILS	Integrated Logistics Support
ISDN	Integrated Services Digital Network
ISME	International Subject Matter Experts
ISO	International Organization for Standardization
ISP	International Standardized Profile
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector

JANAP	Joint Army, Navy, Air Force Procedure
L	Locality
LCC	Local Control Center
LEP	List of Effective Pages
LMF	Language and Media Format
LOP	Letter of Promulgation
MCS	Message Conversion System
MHS	Message Handling System
MIB	Management Information Base
MLA	Mail List Agent
MMHS	Military Message Handling System
MMUA	Military Messaging User Agent
MS	Message Store
MTA	Message Transfer Agent
MTBF	Mean Time Before Failure
MTS	Message Transfer System
MTTR	Mean Time to Repair
NASIS	NATO Subject Indicator System
NATO	North Atlantic Treaty Organization
NAVCOMPARS	Naval Communications Processing and Routing System
NZ	New Zealand
O/R, OR	Originator/Recipient
O	Organization
OSI	Open Systems Interconnection
OU	Organizational Unit

P2	Interpersonal Messaging - 1984 Content Type
P22	Interpersonal Messaging - 1988 Content Type
P772	Military Messaging Content Type
PACOM	Pacific Command
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PLA	Plain Language Address
PRB	Project Review Board
PRMD	Private Management Domain
PSTN	Public Switched Telephone Network
R	GENSER Community
RAN	Release Authority Name
RBAC	Rule-Based Access Control
RDN	Relative Distinguished Name
RFC	Request for Comments
RHOB	Relevant Hierarchical Operational Binding
RI	Routing Indicator
ROSE	Remote Operations Service Element
RTSE	Reliable Transfer Service Element
S/MIME	Secure/Multimedia Internet Mail Extensions
SA	Signal Address
SAC	Simplified Access Control
SDN	Secure Data Network
SHD	Special Handling Designator
SI	Special Intelligence

SIC	Subject Indicator Code
SIGAD	SIGINT Address
SIGINT	Signal Intelligence
SLA	Service Level Agreement
SMIB	Security Management Information Base
SMA	Signal Message Address
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STANAG	Standardization Agreement
STU	Secure Telephone Unit
TARE	Telegraph Automatic Relay Equipment
TCC	Transmission Control Code
TCCG	Transmission Control Code Group
TR	Technical Report
TRC	Transmission Release Code
TSGCE	Tri-Service Group of Communications and Electronics
UA	User Agent
UK	United Kingdom
UKM	User Key Material
US	United States
USMCEB	United States Military Communications-Electronics Board
UTC	Universal Coordinated Time
Y	SI Community



LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers	Change in Effect
Title Page	I (Reverse Blank)	Edition B
Foreword	III (Reverse Blank)	Edition B
Letter of Promulgation	V (Reverse Blank)	Edition B
Record of Changes and Corrections	VII to XVI	Edition B
Record of Pages Checked	XVII, XVIII	Edition B
Table of Contents	XIX to XXIV	Edition B
Chapter 1	1-1 to 1-6	Edition B
Chapter 2	2-1 to 2-20	Edition B
Chapter 3	3-1 to 3-44	Edition B
Chapter 4	4-1 to 4-12	Edition B
Chapter 5	5-1 to 5-4	Edition B
Annex A	A-1 to A-6	Edition B
Annex B	B-i to B-xvi, B-1 to B-170	Edition B
Annex C	C-1 to C-18	Edition B
Annex D	D-i to D-iv, D-1 to D-52	Edition B
Annex E	E-1 to E-6	Edition B
Annex F	F-1 to F-14	Edition B
Annex G	G-1 to G-8	Edition B
List of Effective Pages	LEP-1 to LEP-2	Edition B



