

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.

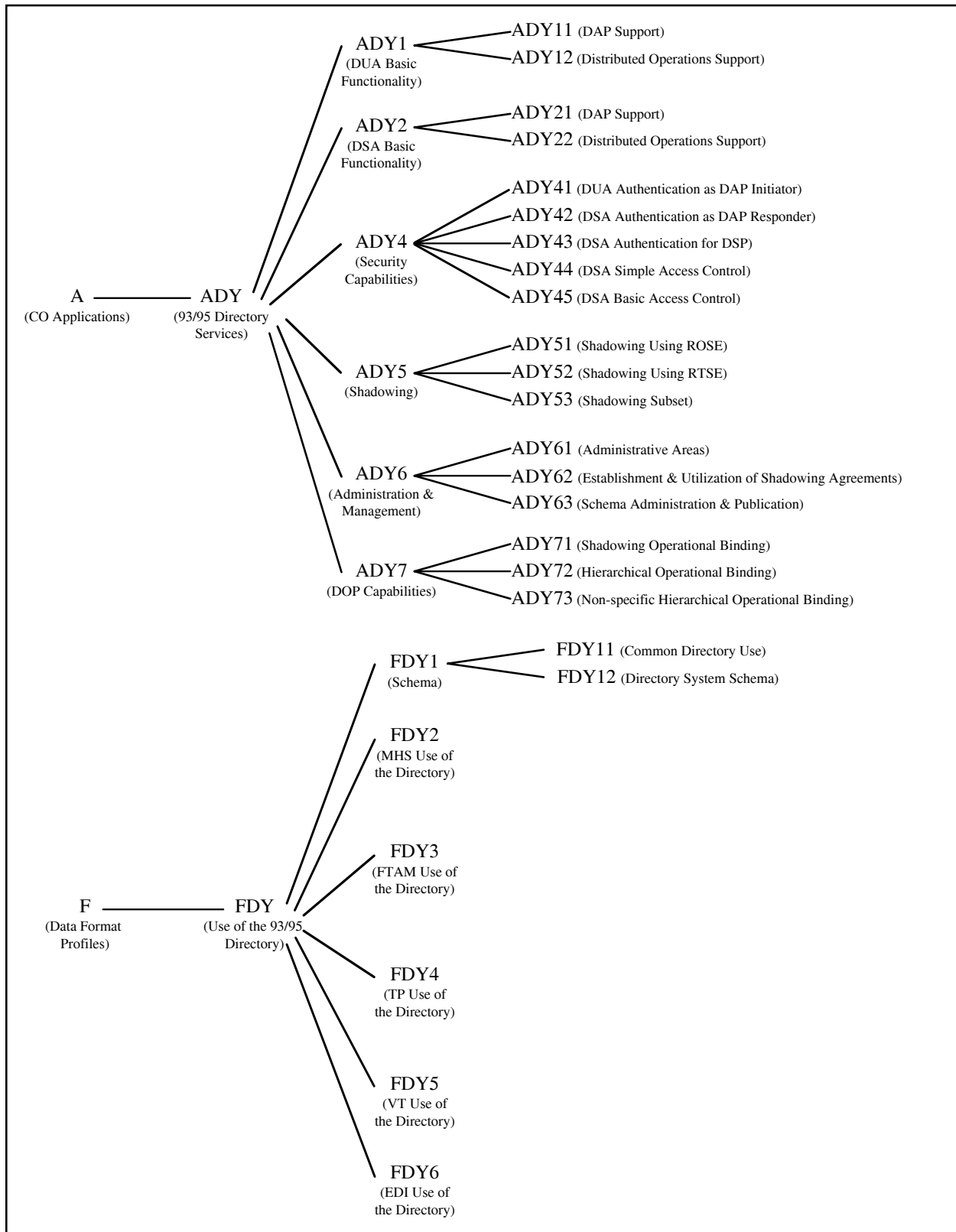


Figure ANNEX C-1
Taxonomy of Directory Functional Profiles

- 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.

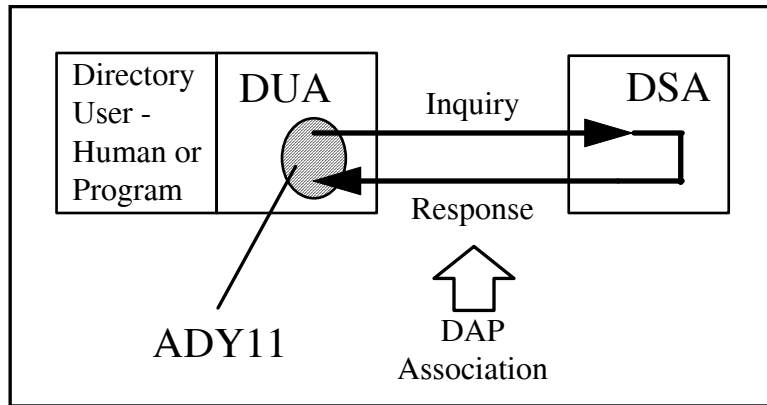


Figure ANNEX C-2
ADY11 Applicability

(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.

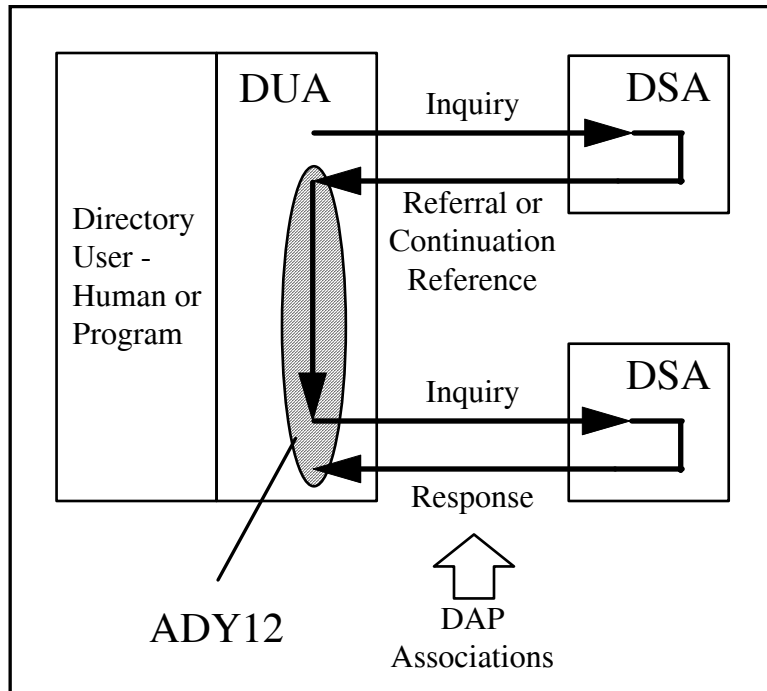


Figure ANNEX C-3
Applicability of ADY12

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 DSA, 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.

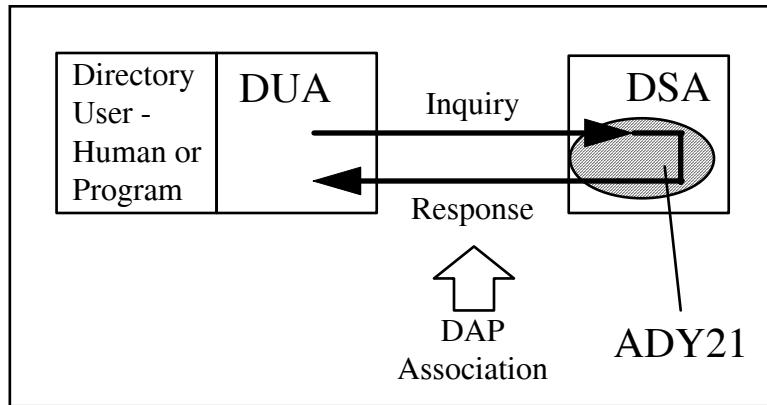


Figure ANNEX C-4
ADY21 Applicability

(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

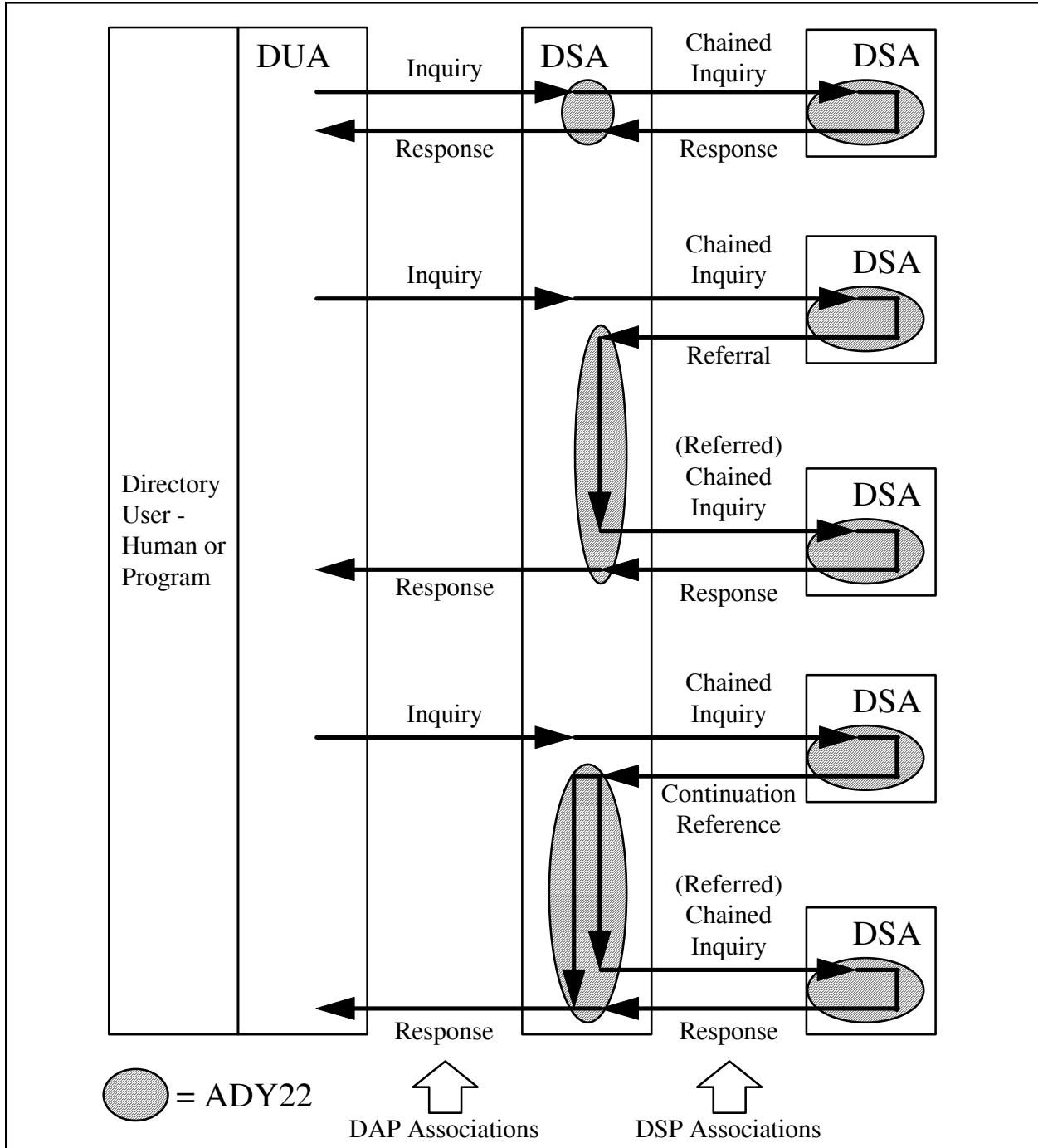


Figure ANNEX C-5
ADY22 Applicability

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.

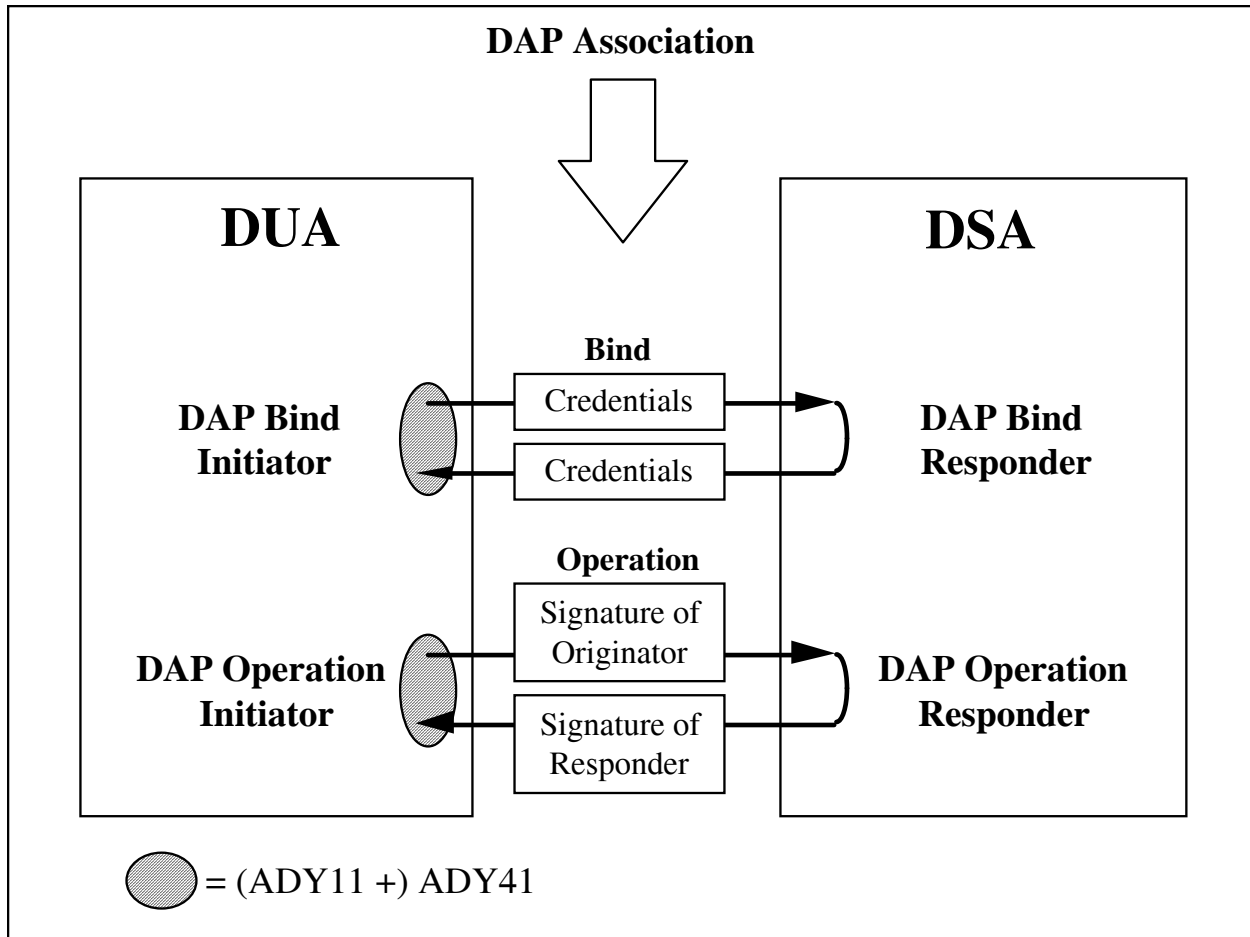


Figure ANNEX C-6
ADY41 Applicability

(2) The ADY42 profile specifies the manner in which a DSA behaves when authenticating a DUA and authenticating itself to a DUA using simple protected authentication or strong authentication as a DAP Responder. It augments the ADY21 requirements with DUA-specific use of authentication beyond simple unprotected binds and use of digitally signed operations (see Figure C-7). ADY42 includes use of different levels of authentication, and of different security infrastructures, e.g., support of hierarchical/non-hierarchical CA structures. In addition, ADY42 covers actions by the DSA on handling (i.e., validating or not) credentials sent by the DUA, the use of two-way strong authentication, procedures for distributed authentication, and digitally signed operations.

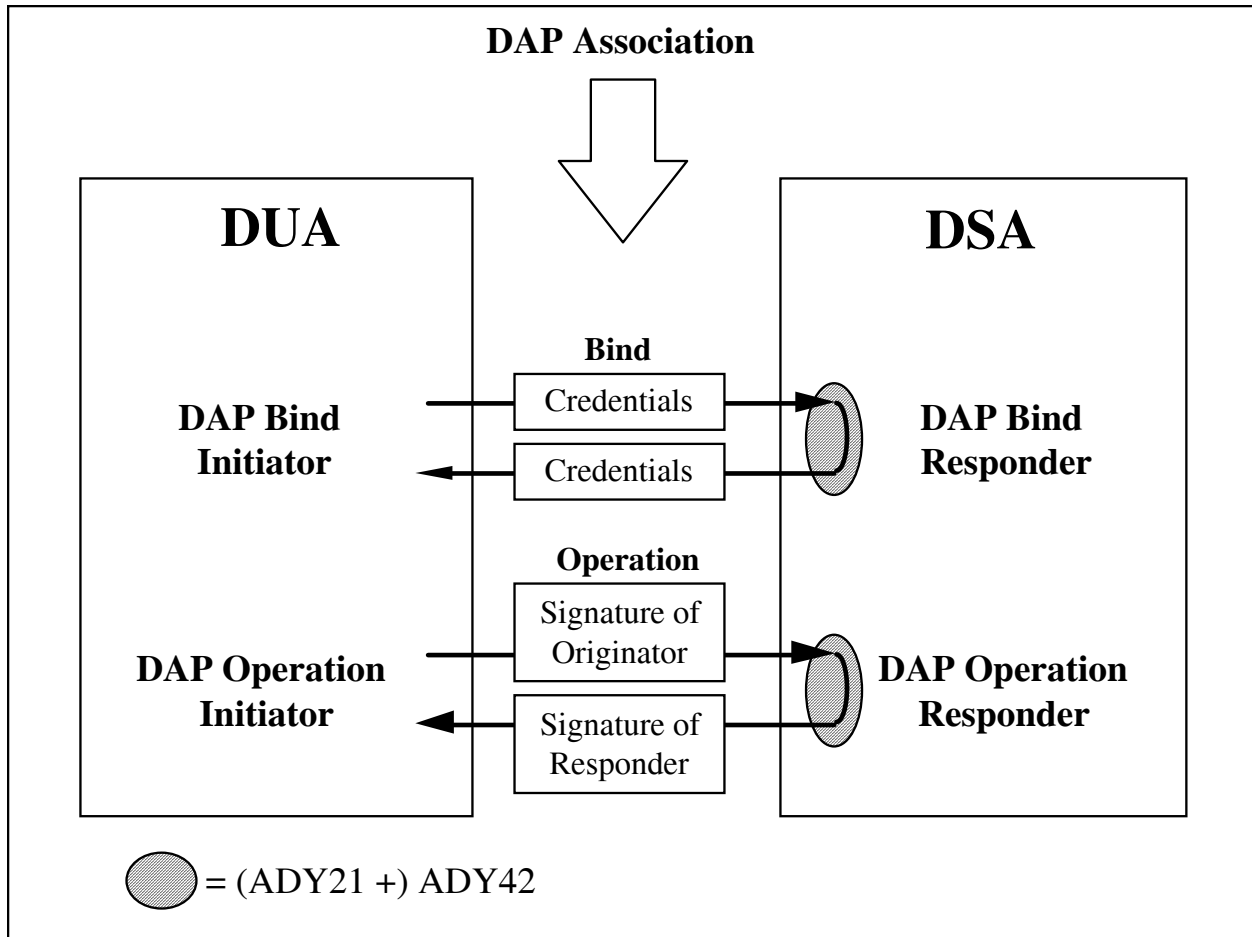


Figure ANNEX C-7
ADY42 Applicability

(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.

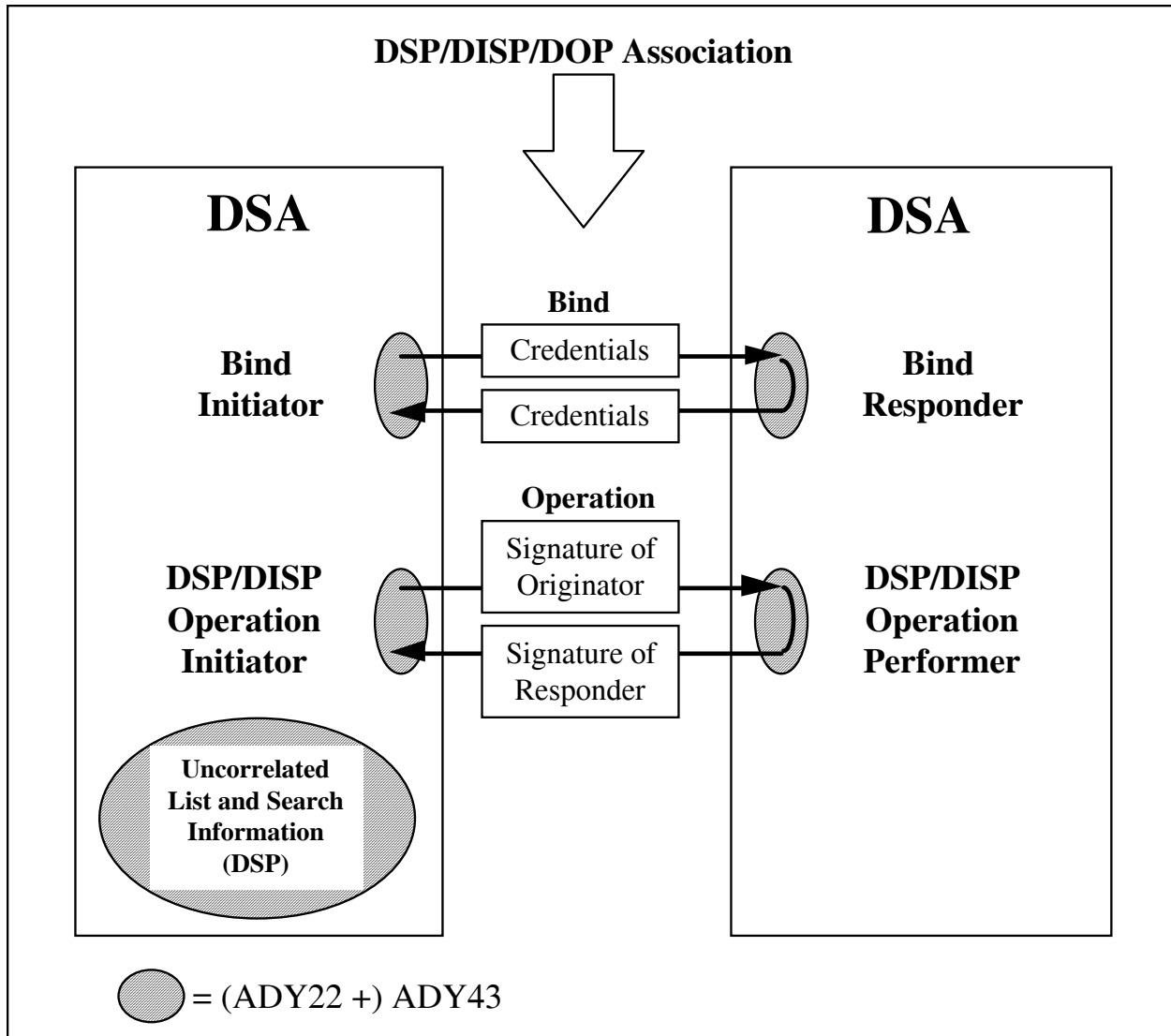


Figure ANNEX C-8
ADY43 Applicability

(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 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). 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 ACItem values of

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

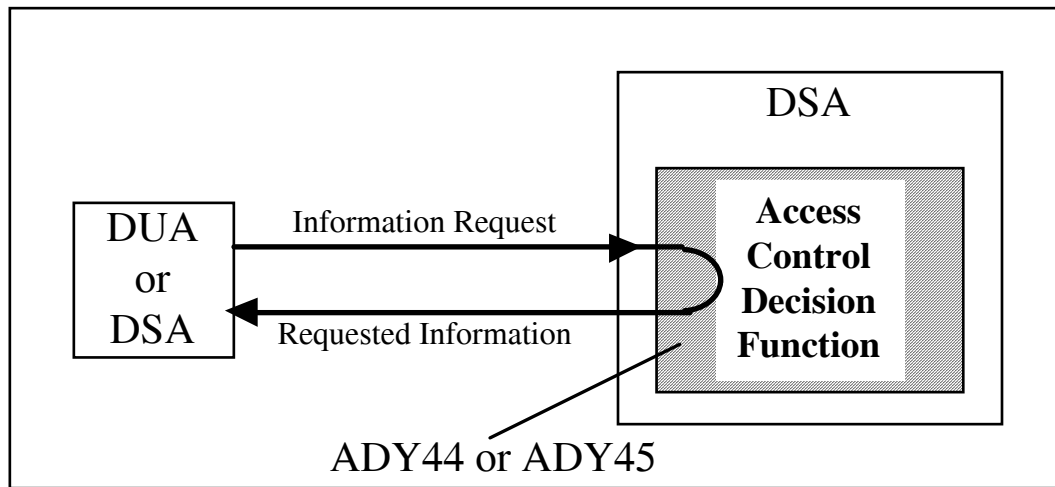


Figure ANNEX C-9
ADY44 or ADY45 Applicability

(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 Utilisation 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.

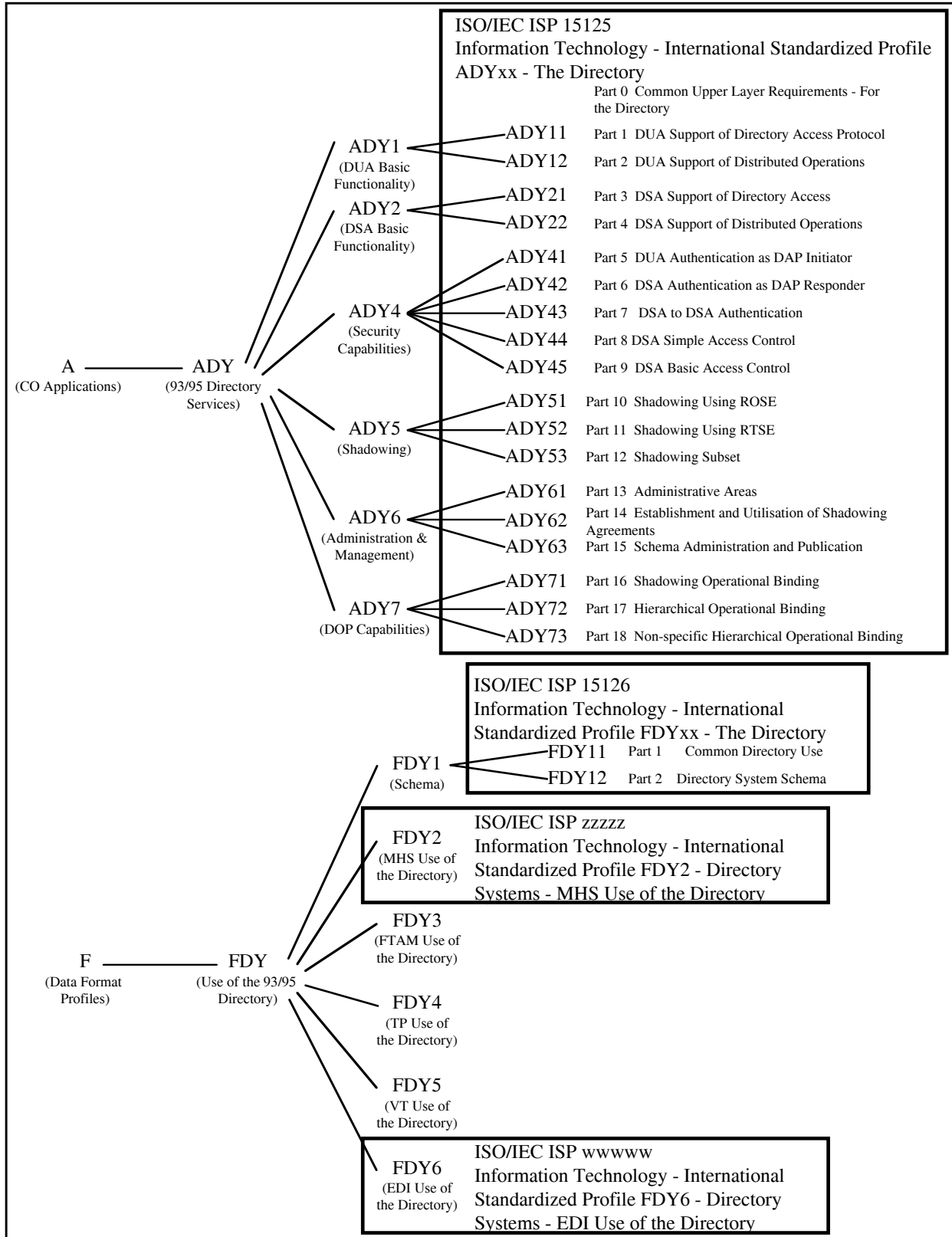


Figure ANNEX C-10
 Organization of Directory Functional Profiles Into International Standardized Profiles

ANNEX DALLIED DIRECTORY SYSTEM FUNCTIONAL PROFILESSECTION IINTRODUCTION1. 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 IIACP 133 ADDITIONS TO CURRENT ISPS AND PICS2. Schemaa. 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 |

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

| Item | Question | D | P | ACP 133 | Predicate |
|------|--|---|------------|------------|------------------|
| 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 | |

Table D-3
X.520 Collective Attribute Types

| Ref. no. | Collective Attribute Type | D & P | ACP 133 | Notes |
|----------|--------------------------------------|-------|------------|-------|
| 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 | |
| 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 | |

Table D-4
Standard Matching Rules

| Ref. no. | Matching Rule | D | P | ACP 133 | Notes |
|----------|------------------------------------|---|---|------------|-------|
| 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 | c2 | 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 | |

Table D-7
Operations

| Item | Operation | D | P | ACP 133 | | | Predicate | Note |
|------|-------------|---|---|---------|---------------|-----|-------------|------|
| | | | | Inter | Inter/ Mod | Adm | | |
| 10 | ModifyEntry | o | o | o | m | m | ModifyEntry | |
| 11 | ModifyDN | o | o | o | m | m | ModifyDN | |

c2: 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 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 | | |

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 | See B6 Signed Operations |

- i. Table D-12 is an adaptation of the table in clause A.4.3.1.1 in ADY41.

Table D-12
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.

- j. Table D-13 contains the differences from clause A.4.3.3.22, Security Parameters.

Table D-13
Security Parameters

| Item No. | Operation | D | P | ACP 133 | | | Predicate | Note |
|----------|--------------------|---|---|---------|-----------|-----|-----------|-----------------------------|
| | | | | Inter | Inter/Mod | Adm | | |
| 1 | certification-path | m | m | o | o | o | | Ref A.4.3.3.23 Note 1 |
| 5 | target | o | o | o | o | o | | Note 2 |

Note 1: The certification path received in the Bind response credentials will be used to validate the signature of the operation response. Therefore, the certification path in the Common Arguments and Chained Arguments SecurityParameters is redundant, and should not be present.

Note 2: The value of ProtectionRequest for 1993 systems shall be 0.

- k. Table D-14 is an adaptation of the table in clause B.3.

Table D-14
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.

1. Table D-15 is an adaptation of the table in clause B.5 in ADY41.

Table D-15
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 | o | c:o | m | m | m | twoWay | |
| 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)

m. Table D-16 is an adaptation of the table in clause B.6 in ADY41.

Table D-16
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-17 contains the differences from clause A.3.1, DSA Implementation and/or System.

Table D-17
DSA Implementation and/or System

| Item No. | Operation | D | P | ACP | Predicate | Note |
|----------|------------------------------|---|---|-----|-----------|------|
| 4a | Cross Reference | o | o | m | | |
| 4c | Immediate Superior Reference | o | o | m | | |

Table D-17
DSA Implementation and/or System

| Item No. | Operation | D | P | ACP | Predicate | Note |
|----------|---|-----|-----|-----|-------------|------|
| 5c | strong | o.1 | o.1 | m | Strong-DSA | |
| 10b | Basic Access Control | o | o | m | BasicAC-DSA | |
| 11 | The DSA support of collective attributes | o | o | m | | |
| 13 | The DSA support of hierarchical attributes | o | o | m | | |
| 14 | The DSA support of auxiliary object classes | o | o | m | | |
| 15 | The DSA support of the subschema for its portion of the DIT | o | o | m | | |

o.1 The DSA must support at least one security level.

(3) 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.

(4) Table D-18 shows the differences from clause A.3 of ADY42.

Table D-18
DSA Implementation and/or System

| Item No. | Operation | D | P | ACP | Reference | Notes |
|----------|--|-----|-----|-----|-------------------|-------|
| 1d | Strong Authentication | o.1 | o.1 | m | strongAuth | |
| 2b | Two-way | o | o | m | twoWay | |
| 3 | Does the DSA support Strong Authentication on Bind Result? | o | o | m | strongBind Result | |
| 4 | Does the DSA support Digitally Signed Operations? | o | o | m | digitalSig | |
| 13 | Does the DSA support Signed Add Entry Request? | o | o | m | signAddReq | |

Table D-18
DSA Implementation and/or System

| Item No. | Operation | D | P | ACP | Reference | Notes |
|----------|--|---|---|-----|--------------------------------|--------|
| 14 | Does the DSA support Signed Remove Entry Request? | o | o | m | signRemoveReq | |
| 15 | Does the DSA support Signed Modify Entry Request? | o | o | m | signModifyReq | |
| 16 | Does the DSA support Signed ModifyDN Request? | o | o | m | signModDNReq | |
| 19 | Does the DSA support strong authentication in the initiator role? | o | o | m | strongAuth | |
| 20 | Does the DSA support strong authentication in the responder role? | o | o | m | strongAuth | |
| 22 | Does the DSA support the generation of certification path for strong authentication? | o | o | m | certPath | |
| 25 | Does the DSA support Authority Revocation List? | o | o | m | arl | |
| 26 | Does the DSA support the ASN.1 Distinguished Encoding Rules (DER)? | o | o | m | strongAuth or digitalSig | Note 2 |

o.1 DSAs must support at least one of protected simple or strong authentication.

Note 2: DSAs shall conform to the encoding rules as specified in [ISO/IEC 9594-8: 1993 | ITU-T Rec. X.509 (1993)] Clause 9.

(5) 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.

(6) Table D-19 shows the differences from clause A.3.1 of ADY45.

Table D-19
DSA implementation and/or system

| Item No. | Question | D | P | ACP | Predicate | Note |
|----------|--|---|-----|-----|------------------------------|------|
| 2b | Supported Access Controls : Basic Access Control | o | o.2 | m | BAC-DSA | |
| 5b | Supported application contexts: directorySystemAC | o | o | m | chainingDSA | |
| 12 | Does the DSA support Import for entry access? | o | o | m | importEntry | |
| 13 | Does the DSA support Export for entry access? | o | o | m | exportEntry | |
| 14 | Does the DSA support ReturnDN for entry access? | o | o | m | returnDNEntry | |
| 15 | Does the DSA support DiscloseOnError for entry access? | o | o | m | | |
| 21 | Does the DSA support DiscloseOnError for attribute access? | o | o | m | discloseOnError Attribute | |

o.2 The DSA must support at least one of SAC or BAC to be conformant to this ISP.

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-20 shows the differences from clause A.3.1 of ADY22.

Table D-20
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 |
| 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 |

Table D-20
DSA implementation and/or system

| Item No. | Question | D | P | ACP | Predicate Name or note |
|----------|---|---|---|-----|------------------------|
| 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.

(4) Table D-21 specifies the differences from clause A.3.1, Global statement of conformance - DSP.

Table D-21
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 |

Table D-21
Global Statement of Conformance - DSP

| Item No. | Question | D | P | ACP | Predicate Name or note |
|----------|--|---|---|-----|------------------------|
| 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-22 specifies the differences from clause A.3.4, Global statement of conformance - all supported protocols.

Table D-22
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-23 specifies the differences from clause A.3.1, General Capabilities.

Table D-23
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? | o | o | 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 |

(7) DSAs shall conform to ISO/IEC ISP 15125-9 (ADY45). See Table D-19.

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-24 specifies the differences from clause A.3.3, Global statement of conformance - DISP.

Table D-24
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 |
| 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-22 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-25 specifies the differences from clause A.3 of ADY51.

Table D-25
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-26 specifies the differences from clause A.3.1 of ADY53.

Table D-26
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_e cp = 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-27 specifies the differences from clause A.3.2, Global statement of conformance - DOP.

Table D-27
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 |
| 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-22 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-28 specifies the differences from clause 6 of ADY72.

Table D-28
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 III

DUA EXTENSIONS

5. Administrative DUAs

a. Because of the variety of DUAs, FDY12 does not include any tables for DUAs. Table D-29 identifies support required for ACP 133 A DUAs, 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-29
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-30 shows the standard object classes that shall be supported by ADUAs.

Table D-30
Standard Operational Object Classes - Administrative DUAs

| Item | Object Class | D | ACP 133 | Notes |
|------|-----------------------------|---|------------|-------|
| 1 | subentry | m | C4 | |
| 2 | subschemaSubentry | o | C1 | |
| 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-31 shows the attribute types, defined in X.500 (1993), that shall be supported by ADUAs.

Table D-31
Standard Operational Attribute Types - Administrative DUAs

| Item | Attribute Type | D | AC P 133 | Notes |
|------|-----------------|---|----------------|-------|
| 1 | createTimeStamp | m | m | |
| 2 | modifyTimeStamp | o | m | |
| 3 | creatorsName | o | m | |
| 4 | modifiersName | o | m | |

Table D-31
Standard Operational Attribute Types - Administrative DUAs

| Item | Attribute Type | D | AC P 133 | Notes |
|------|------------------------|---|----------------|-------|
| 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 | |
| 19 | entryACI | o | C3 | |
| 20 | subentryACI | o | C3 | |
| 21 | dseType | o | m | |
| 22 | myAccessPoint | o | m | |
| 23 | superiorKnowledge | o | m | |
| 24 | specificKnowledge | o | m | |

Table D-31
Standard Operational Attribute Types - Administrative DUAs

| Item | Attribute Type | D | AC P 133 | Notes |
|------|----------------------|---|----------------|-------|
| 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. Table D-32 shows the object classes, defined in X.402, that shall be supported.

Table D-32
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 | | |

b. Table D-33 shows the object classes, defined in this ACP, that shall be supported.

Table D-33
ACP 133 Object Classes

| Item | Object Class | ACP 133 | Notes | PICS Response |
|------|-----------------------------|------------|-------|------------------|
| 1 | addressList | m | | |
| 2 | aliasCommonName | m | | |
| 3 | aliasOrganizationalUnit | m | | |
| 4 | altSpellingACP127 | m | | |
| 5 | cadACP127 | m | | |
| 6 | distributionCodeDescription | m | | |
| 7 | distributionCodesHandled | m | | |
| 8 | messagingGateway | m | | |
| 9 | mLA | m | | |

Table D-33
ACP 133 Object Classes

| Item | Object Class | ACP 133 | Notes | PICS Response |
|------|-------------------------|------------|-------|------------------|
| 10 | network | m | | |
| 11 | networkInstructions | m | | |
| 12 | orgACP127 | m | | |
| 13 | otherContactInformation | m | | |
| 14 | plaACP127 | m | | |
| 15 | plaCollectiveACP127 | m | | |
| 16 | plaData | m | | |
| 17 | plaUser | m | | |
| 18 | releaseAuthorityPerson | m | | |
| 19 | routingIndicator | m | | |
| 20 | secure-user | m | | |
| 21 | sigintPLA | m | | |
| 22 | sIPLA | m | | |
| 23 | spotPLA | m | | |
| 24 | taskForceACP127 | m | | |
| 25 | tenantACP127 | m | | |
| 26 | ukms | m | | |

c. Table D-34 shows the object classes, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-34
1997 Standard Object Classes

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

d. Table D-35 shows the attribute types, defined in X.402, that shall be supported.

Table D-35
X.402 Attribute Types

| Item | Attribute Type | D | AC P 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 | | |

Table D-35
X.402 Attribute Types

| Item | Attribute Type | D | AC P 133 | Notes | PICS Response |
|------|------------------------------------|---|----------------|-------|------------------|
| 12 | mhs-message-store-dn | o | m | | |
| 13 | mhs-or-addresses | o | m | | |
| 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 | | |

e. Table D-36 shows the attribute types, defined in this ACP, that shall be supported.

Table D-36
ACP 133 Attribute Types

| Item | Attribute Type | ACP 133 | Notes | PICS Response |
|------|--------------------------|------------|-------|------------------|
| 1 | accessCodes | m | | |
| 2 | accessSchema | m | | |
| 3 | accountingCode | m | | |
| 4 | aCPMobileTelephoneNumber | m | | |
| 5 | aCPPagerTelephoneNumber | m | | |

Table D-36
ACP 133 Attribute Types

| Item | Attribute Type | ACP 133 | Notes | PICS Response |
|------|---------------------------------|------------|-------|------------------|
| 6 | aCPPreferredDelivery | m | | |
| 7 | aCPTelephoneFacsimileNumber | m | | |
| 8 | actionAddressees | m | | |
| 9 | additionalAddressees | m | | |
| 10 | additionalSecondPartyAddressees | m | | |
| 11 | administrator | m | | |
| 12 | aigsExpanded | m | | |
| 13 | aLExemptedAddressProcessor | m | | |
| 14 | aliasPointer | m | | |
| 15 | alid | m | | |
| 16 | allowableOriginators | m | | |
| 17 | aLReceiptPolicy | m | | |
| 18 | alternateRecipient | m | | |
| 19 | alType | m | | |
| 20 | aprUKMs | m | | |
| 21 | associatedAL | m | | |
| 22 | associatedOrganization | m | | |
| 23 | associatedPLA | m | | |
| 24 | augUKMs | m | | |
| 25 | cognizantAuthority | m | | |
| 26 | community | m | | |

Table D-36
ACP 133 Attribute Types

| Item | Attribute Type | ACP 133 | Notes | PICS Response |
|------|------------------------|------------|-------|------------------|
| 27 | copyMember | m | | |
| 28 | decUKMs | m | | |
| 29 | distributionCodeAction | m | | |
| 30 | distributionCodeInfo | m | | |
| 31 | dualRoute | m | | |
| 32 | effectiveDate | m | | |
| 33 | entryClassification | m | | |
| 34 | expirationDate | m | | |
| 35 | febUKMs | m | | |
| 36 | gatewayType | m | | |
| 37 | ghpType | m | | |
| 38 | guard | m | | |
| 39 | hostOrgACP127 | m | | |
| 40 | infoAddressees | m | | |
| 41 | janUKMs | m | | |
| 42 | julUKMs | m | | |
| 43 | junUKMs | m | | |
| 44 | lastRecapDate | m | | |
| 45 | listPointer | m | | |
| 46 | lmf | m | | |
| 47 | longTitle | m | | |

Table D-36
ACP 133 Attribute Types

| Item | Attribute Type | ACP 133 | Notes | PICS Response |
|------|-------------------------|------------|-------|------------------|
| 48 | mailDomains | m | | |
| 49 | marUKMs | m | | |
| 50 | mayUKMs | m | | |
| 51 | militaryFacsimileNumber | m | | |
| 52 | militaryTelephoneNumber | m | | |
| 53 | nameClassification | m | | |
| 54 | nationality | m | | |
| 55 | networkDN | m | | |
| 56 | networkSchema | m | | |
| 57 | novUKMs | m | | |
| 58 | octUKMs | m | | |
| 59 | onSupported | m | | |
| 60 | operationName | m | | |
| 61 | plaAddressees | m | | |
| 62 | plaNNameACP127 | m | | |
| 63 | plaReplace | m | | |
| 64 | positionNumber | m | | |
| 65 | primarySpellingACP127 | m | | |
| 66 | proprietaryMailboxes | m | | |
| 67 | publish | m | | |
| 68 | rank | m | | |

Table D-36
ACP 133 Attribute Types

| Item | Attribute Type | ACP 133 | Notes | PICS Response |
|------|-----------------------|------------|-------|------------------|
| 69 | recapDueDate | m | | |
| 70 | releaseAuthorityName | m | | |
| 71 | remarks | m | | |
| 72 | rI | m | | |
| 73 | rIClassification | m | | |
| 74 | rIInfo | m | | |
| 75 | secondPartyAddressees | m | | |
| 76 | section | m | | |
| 77 | secureFacsimileNumber | m | | |
| 78 | secureTelephoneNumber | m | | |
| 79 | sepUKMs | m | | |
| 80 | serviceNumber | m | | |
| 81 | serviceOrAgency | m | | |
| 82 | sHD | m | | |
| 83 | shortTitle | m | | |
| 84 | sigad | m | | |
| 85 | spot | m | | |
| 86 | tARE | m | | |
| 87 | tCC | m | | |
| 88 | transferStation | m | | |
| 89 | tRC | m | | |

f. Table D-37 shows the attribute types, defined in RFC 1274, that shall be supported.

Table D-37
RFC 1274 Attribute Types

| Item | Attribute Type | AC P 133 | Notes | PICS Response |
|------|----------------|----------------|-----------------------|------------------|
| 1 | host | m | | |
| 2 | rfc822Mailbox | m | also known as mail | |
| 3 | roomNumber | m | | |

g. Table D-38 shows the attribute types, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-38
1997 Standard Attribute Types

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

h. Table D-39 shows the collective attribute types, defined in this ACP, that shall be supported.

Table D-39
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 | | |

- i. Table D-40 shows the name forms, defined in this ACP, that shall be supported.

Table D-40
ACP 133 Name Forms

| Item | Name Form | D & P | ACP 133 | Notes | PICS Response |
|------|-------------------------------------|-------|------------|-------|------------------|
| 1 | addressListNameForm | - | m | | |
| 2 | aENameForm | - | m | | |
| 3 | aliasCNNameForm | - | m | | |
| 4 | aliasOUNameForm | - | m | | |
| 5 | alternateSpellingPLANameForm | - | m | | |
| 6 | cadPLANameForm | - | m | | |
| 7 | distributionCodeDescriptionNameForm | - | m | | |
| 8 | messagingGatewayNameForm | - | m | | |

Table D-40
ACP 133 Name Forms

| Item | Name Form | D & P | ACP 133 | Notes | PICS Response |
|------|--------------------------------|-------|------------|-------|------------------|
| 9 | mhs-dLNameForm | - | m | | |
| 10 | mLANameForm | - | m | | |
| 11 | mSNameForm | - | m | | |
| 12 | mTANameForm | - | m | | |
| 13 | mUANameForm | - | m | | |
| 14 | networkNameForm | - | m | | |
| 15 | networkInstructionsNameForm | - | m | | |
| 16 | organizationalPLANameForm | - | m | | |
| 17 | organizationNameForm | - | m | | |
| 18 | orgRNameForm | - | m | | |
| 19 | orgUNameForm | - | m | | |
| 20 | plaCollectiveNameForm | - | m | | |
| 21 | qualifiedOrgPersonNameForm | - | m | | |
| 22 | releaseAuthorityPersonNameForm | - | m | | |
| 23 | routingIndicatorNameForm | - | m | | |
| 24 | sigintPLANameForm | - | m | | |
| 25 | siPLANameForm | - | m | | |
| 26 | spotPLANameForm | - | m | | |
| 27 | taskForcePLANameForm | - | m | | |
| 28 | tenantPLANameForm | - | m | | |

j. Table D-41 shows the name forms, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-41
1997 Standard Name Forms

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

k. Table D-42 shows the matching rules, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-42
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.

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

7. DUA Extensions

- a. Table D-43 contains the 1997 additions to Security Parameters for DUAs.

Table D-43
1997 Additions to Security Parameters

| Item | Operation | D | ACP 133 | | | Predicate | Note | PICS Response |
|------|--------------------------------|---|---------|-----------|-----|-----------|------|---------------|
| | | | Inter | Inter/Mod | Adm | | | |
| 1 | response | o | o | m | m | | | |
| 2 | operationCode | o | o | o | o | | | |
| 3 | attribute CertificationPath | o | o | o | o | | | |
| 4 | errorProtection | o | o | o | o | | | |

- b. Table D-44 contains the additional Directory Bind Arguments elements, defined in the 1997 edition of the Directory standards, that shall be supported by DUAs.

Table D-44
1997 Directory Bind Arguments

| Item | Operation | D | ACP 133 | | | Predicate | Note | PICS Response |
|------|-----------|---|---------|-----------|-----|-----------|------|---------------|
| | | | Inter | Inter/Mod | Adm | | | |
| 1 | response | o | m | m | m | | | |

8. DSA Extensions

- a. DAP

- (1) Table D-45 contains the 1997 additions to Security Parameters for DSAs.

Table D-45
1997 Additions to Security Parameters

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|--------------------------------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |
| 2 | operationCode | o | o | | | |
| 3 | attribute CertificationPath | o | o | | | |
| 4 | errorProtection | o | o | | | |

(2) Table D-46 contains the additional Directory Bind Arguments elements, defined in the 1997 edition of the Directory standards, that shall be supported.

Table D-46
1997 Directory Bind Arguments

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|-----------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |

b. DSP

(1) Table D-47 contains the 1997 additions to Security Parameters.

Table D-47
1997 Additions to Security Parameters

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|--------------------------------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |
| 2 | operationCode | o | o | | | |
| 3 | attribute CertificationPath | o | o | | | |
| 4 | errorProtection | o | o | | | |

(2) Table D-48 contains the additional Directory Bind Arguments elements, defined in the 1997 edition of the Directory standards, that shall be supported.

Table D-48
1997 Directory Bind Arguments

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|-----------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |

c. DISP

Table D-49 contains the additional Directory Bind Arguments elements, defined in the 1997 edition of the Directory standards, that shall be supported.

Table D-49
1997 Directory Bind Arguments

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|-----------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |

d. DOP

Table D-50 contains the additional Directory Bind Arguments elements, defined in the 1997 edition of the Directory standards, that shall be supported.

Table D-50
1997 Directory Bind Arguments

| Item | Operation | D | ACP 133 | Predicate | Note | PICS Response |
|------|-----------|---|------------|-----------|------|------------------|
| 1 | response | o | m | | | |

ANNEX EEXAMPLE SHADOWING AGREEMENT

Table ANNEX 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 |
| Supplier DSA (SD) | |
| 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: | |
| Consumer DSA (CD) | |
| 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: |
| |
| Agreements |
| 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: _____ _____ |

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.

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

| | Section | Issue | Date of Issue | Remarks |
|---------------|-----------------------------------|--------------|----------------------|----------------|
| 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

| COPY NUMBER | HOLDER | LOCATION |
|--------------------|---------------|-----------------|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |

CONTENTS

DEFINITIONS

| | |
|-----------------------------|--|
| Services | The provision of planning, procurement, implementation, change control, task co-ordination, project management, configuration management, maintenance, security, documentation, operator services, quality control, and financial management of <assets> within the <organisation> 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 timescales.

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)

| SERVICE ATTRIBUTES | SERVICE OPTION No. | SERVICE OPTION DESCRIPTION |
|---|---------------------------|---|
| FEATURES | 1a | |
| | 1b | |
| SECURITY | 2a | UNCLASSIFIED |
| | 2b | RESTRICTED |
| | 2c | SECRET |
| MANAGEMENT | 3a | No Control or Monitoring |
| | 3b | Central Control and Monitoring |
| | 3c | |
| | 3d | Local control only |
| SURVIVABILITY | 4a | Standard |
| | 4b | Physical security |
| | 4c | Blast protected |
| | 4d | EMP protected |
| | 4e | Route Diversity |
| INTERFACES | 6a | |
| | 6b | |
| PERFORMANCE | 7 | |
| PERFORMANCE (Site Service Availability measured over 1 year) | 7a | x% |
| | 7b | x% |
| PERFORMANCE (Grade of Service) | 7d | |
| SYNCHRONIZATION | | |
| MAINTENANCE | 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> timescales. 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 timescales for the three categories as shown below:

| Category | Timescale |
|----------------------|--|
| Operational | <Two days> Earlier timescale, if achievable, to be agreed within 24 hours of receipt |
| Priority | <Five days> Earlier timescale, if achievable, to be agreed within 24 hours of receipt |
| Normal (baseline) | |

25. 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

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

MEETINGS

27. <As Appropriate>

APPENDIX C - MANAGEMENT POINTS OF CONTACT

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

Hour by Hour Management

| Service Provider | Customer |
|---------------------------|-----------------|
| Help Desks: | |
| System Supervisor: | |

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 |
| DAP | Directory Access Protocol |
| DFTS | Defence 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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) | Original |
| Foreword | III (Reverse Blank) | Original |
| Letter of Promulgation | V (Reverse Blank) | Original |
| Record of Changes and Corrections | VII, VIII | Original |
| Record of Pages Checked | IX, X | Original |
| Table of Contents | XII to XVI | Original |
| Chapter 1 | 1-1 to 1-6 | Original |
| Chapter 2 | 2-1 to 2-18 | Original |
| Chapter 3 | 3-1 to 3-44 | Original |
| Chapter 4 | 4-1 to 4-12 | Original |
| Chapter 5 | 5-1 to 5-4 | Original |
| Annex A | A-1 to A-6 | Original |
| Annex B | B-i to B-xii, B-1 to B-160 | Original |
| Annex C | C-1 to C-16 | Original |
| Annex D | D-1 to D-44 | Original |
| Annex E | E-1 to E-4 | Original |
| Annex F | F-1 to F-14 | Original |
| Annex G | G-1 to G-6 | Original |
| List of Effective Pages | LEP-1 to LEP-2 | Original |

