Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14155
Date:	2009-12-14
Replaces:	
Document Type:	Working Draft
Document Title:	Working Draft of ISO/IEC 9594-All, 2008 OSI - The Directory – WD: Communications support enhancements, X.500 Series of Recommendations (2008)
Document Source:	JTC1/ITU-T Geneva meeting
Project Number:	
Document Status:	SC 6 NBs are requested to submit comments on this WD, if any no later than 14 January 2010.
Action ID:	COM
Due Date:	2010-01-14
No. of Pages:	149

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

TITLE: X.500 Series of Recommendations (2008) | ISO/IEC 9594-All : 2008 OSI - The Directory – WD: Communications support enhancements

SOURCE: Collaborative ITU-T and ISO/IEC JTC1 meeting on the Directory, Geneva, Switzerland, 16–25 September 2009

Contents

ISO/IEC 9594-1 : 2008, Information Technology - Open systems Interconnection - The Directory: Overview of concepts, models and services

Working draft for Amendment 1: Communications support enhancements

No change

ISO/IEC 9594-2 : 2008, Information Technology - Open systems Interconnection - The Directory: Models

Working draft for Amendment 1: Communications support enhancements

Annex A

Object identifier usage

Replace the ASN.1 module in Annex A with the following

```
UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 6}
DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
-- modules contained within these Directory Specifications, and for the use of other
-- applications which will use them to access Directory services. Other applications
-- may use them for their own purposes, but this will not constrain extensions and
-- modifications needed to maintain or improve the Directory service.

ID    ::= OBJECT IDENTIFIER

ds ID ::= {joint-iso-itu-t ds(5)}

-- categories of information object

module                                  ID ::= {ds 1}
serviceElement                          ID ::= {ds 2}
applicationContext                      ID ::= {ds 3}
attributeType                           ID ::= {ds 4}
attributeSyntax                         ID ::= {ds 5}
objectClass                             ID ::= {ds 6}
-- attributeSet                         ID ::= {ds 7}
algorithm                               ID ::= {ds 8}
abstractSyntax                          ID ::= {ds 9}
-- object                               ID ::= {ds 10}
-- port                                 ID ::= {ds 11}
dsaOperationalAttribute                 ID ::= {ds 12}
matchingRule                            ID ::= {ds 13}
knowledgeMatchingRule                   ID ::= {ds 14}
nameForm                                ID ::= {ds 15}
group                                   ID ::= {ds 16}
subentry                                ID ::= {ds 17}
operationalAttributeType                ID ::= {ds 18}
operationalBinding                      ID ::= {ds 19}
schemaObjectClass                       ID ::= {ds 20}
schemaOperationalAttribute              ID ::= {ds 21}
administrativeRoles                     ID ::= {ds 23}
accessControlAttribute                  ID ::= {ds 24}
--rosObject                            ID ::= {ds 25}
--contract                             ID ::= {ds 26}
--package                              ID ::= {ds 27}
accessControlSchemes                    ID ::= {ds 28}
certificateExtension                    ID ::= {ds 29}
managementObject                        ID ::= {ds 30}
attributeValueContext                   ID ::= {ds 31}
-- securityExchange                     ID ::= {ds 32}
idmProtocol                             ID ::= {ds 33}
problem                                 ID ::= {ds 34}
notification                            ID ::= {ds 35}
```

```
matchingRestriction                     ID ::= {ds 36} -- None are currently defined
controlAttributeType                    ID ::= {ds 37}
keyPurposes                             ID ::= {ds 38}

-- modules

usefulDefinitions                       ID ::= {module usefulDefinitions(0) 6}
informationFramework                    ID ::= {module informationFramework(1) 6}
directoryAbstractService                ID ::= {module directoryAbstractService(2) 6}
distributedOperations                   ID ::= {module distributedOperations(3) 6}
-- protocolObjectIdentifiers            ID ::= {module protocolObjectIdentifiers(4) 6}
selectedAttributeTypes                  ID ::= {module selectedAttributeTypes(5) 6}
selectedObjectClasses                   ID ::= {module selectedObjectClasses(6) 6}
authenticationFramework                 ID ::= {module authenticationFramework(7) 6}
algorithmObjectIdentifiers              ID ::= {module algorithmObjectIdentifiers(8) 6}
directoryObjectIdentifiers              ID ::= {module directoryObjectIdentifiers(9) 6}
-- upperBounds                          ID ::= {module upperBounds(10) 6}
-- dap                                  ID ::= {module dap(11) 6}
-- dsp                                  ID ::= {module dsp(12) 6}
distributedDirectoryOIDs                ID ::= {module distributedDirectoryOIDs(13) 6}
directoryShadowOIDs                     ID ::= {module directoryShadowOIDs(14) 6}
directoryShadowAbstractService          ID ::= {module
                                            directoryShadowAbstractService(15) 6}
-- disp                                 ID ::= {module disp(16) 6}
-- dop                                  ID ::= {module dop(17) 6}
opBindingManagement                     ID ::= {module opBindingManagement(18) 6}
opBindingOIDs                           ID ::= {module opBindingOIDs(19) 6}
hierarchicalOperationalBindings         ID ::= {module
                                            hierarchicalOperationalBindings(20) 6}
dsaOperationalAttributeTypes            ID ::= {module
                                            dsaOperationalAttributeTypes(22) 6}
schemaAdministration                    ID ::= {module schemaAdministration(23) 6}
basicAccessControl                      ID ::= {module basicAccessControl(24) 6}
directoryOperationalBindingTypes        ID ::= {module
                                            directoryOperationalBindingTypes(25) 6}
certificateExtensions                   ID ::= {module certificateExtensions(26) 6}
directoryManagement                     ID ::= {module directoryManagement(27) 6}
enhancedSecurity                        ID ::= {module enhancedSecurity(28) 6}
-- directorySecurityExchanges           ID ::= {module
--                                          directorySecurityExchanges (29) 6}
iDMProtocolSpecification                ID ::= {module iDMProtocolSpecification(30) 6}
directoryIDMProtocols                   ID ::= {module directoryIDMProtocols(31) 6}
attributeCertificateDefinitions         ID ::= {module
attributeCertificateDefinitions(32) 6}
serviceAdministration                   ID ::= {module serviceAdministration(33) 6}
-- the following definition is for a module that holds externally defined schema elements
-- not defined using formal ASN.1 notation
externalDefinitions                     ID ::= {module externalDefinitions(34) 6}
commonProtocolSpecification             ID ::= {module
                                            commonProtocolSpecification(35) 6}
oSIProtocolSpecification                ID ::= {module oSIProtocolSpecification(36) 6}
directoryOSIProtocols                   ID ::= {module directoryOSIProtocols(37) 6}

-- synonyms

id-oc                                   ID ::= objectClass
id-at                                   ID ::= attributeType
id-as                                   ID ::= abstractSyntax
id-mr                                   ID ::= matchingRule
id-nf                                   ID ::= nameForm
id-sc                                   ID ::= subentry
id-oa                                   ID ::= operationalAttributeType
id-ob                                   ID ::= operationalBinding
id-doa                                  ID ::= dsaOperationalAttribute
id-kmr                                  ID ::= knowledgeMatchingRule
id-soc                                  ID ::= schemaObjectClass
id-soa                                  ID ::= schemaOperationalAttribute
id-ar                                   ID ::= administrativeRoles
```

```
id-aca                                  ID ::= accessControlAttribute
id-ac                                   ID ::= applicationContext
-- id-rosObject                         ID ::= rosObject
-- id-contract                          ID ::= contract
-- id-package                           ID ::= package
id-acScheme                             ID ::= accessControlSchemes
id-ce                                   ID ::= certificateExtension
id-mgt                                  ID ::= managementObject
id-avc                                  ID ::= attributeValueContext
-- id-se                                ID ::= securityExchange
id-idm                                  ID ::= idmProtocol
id-pr                                   ID ::= problem
id-not                                  ID ::= notification
id-mre                                  ID ::= matchingRestriction
id-cat                                  ID ::= controlAttributeType
id-kp                                   ID ::= keyPurposes

-- obsolete module identifiers

-- usefulDefinition                     ID ::= {module 0}
-- informationFramework                 ID ::= {module 1}
-- directoryAbstractService             ID ::= {module 2}
-- distributedOperations                ID ::= {module 3}
-- protocolObjectIdentifiers            ID ::= {module 4}
-- selectedAttributeTypes               ID ::= {module 5}
-- selectedObjectClasses                ID ::= {module 6}
-- authenticationFramework              ID ::= {module 7}
-- algorithmObjectIdentifiers           ID ::= {module 8}
-- directoryObjectIdentifiers           ID ::= {module 9}
-- upperBounds                          ID ::= {module 10}
-- dap                                  ID ::= {module 11}
-- dsp                                  ID ::= {module 12}
-- distributedDirectoryObjectIdentifiers ID ::= {module 13}

-- unused module identifiers

-- directoryShadowOIDs                  ID ::= {module 14}
-- directoryShadowAbstractService       ID ::= {module 15}
-- disp                                 ID ::= {module 16}
-- dop                                  ID ::= {module 17}
-- opBindingManagement                  ID ::= {module 18}
-- opBindingOIDs                        ID ::= {module 19}
-- hierarchicalOperationalBindings      ID ::= {module 20}
-- dsaOperationalAttributeTypes         ID ::= {module 22}
-- schemaAdministration                 ID ::= {module 23}
-- basicAccessControl                   ID ::= {module 24}
-- operationalBindingOIDs               ID ::= {module 25}

END -- UsefulDefinitions
```

Annex B

Information Framework in ASN.1

Replace the ASN.1 module in Annex B with the following

```
InformationFramework {joint-iso-itu-t ds(5) module(1) informationFramework(1) 6}
DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
```

```
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.

IMPORTS

  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2

  directoryAbstractService, id-ar, id-at, id-mr, id-nf, id-oa, id-oc,
  id-sc, selectedAttributeTypes, serviceAdministration
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)usefulDefinitions(0) 6}

  SearchRule
    FROM ServiceAdministration serviceAdministration

  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3

  TypeAndContextAssertion
    FROM DirectoryAbstractService directoryAbstractService

  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6

  booleanMatch, commonName, generalizedTimeMatch, generalizedTimeOrderingMatch,
  integerFirstComponentMatch, integerMatch, integerOrderingMatch,
  objectIdentifierFirstComponentMatch, UnboundedDirectoryString
    FROM SelectedAttributeTypes selectedAttributeTypes;

-- attribute data types

Attribute{ATTRIBUTE:SupportedAttributes} ::= SEQUENCE {
  type                ATTRIBUTE.&id({SupportedAttributes}),
  values              SET SIZE (0..MAX) OF ATTRIBUTE.&Type({SupportedAttributes}{@type}),
  valuesWithContext   SET SIZE (1..MAX) OF       SEQUENCE {
    value               ATTRIBUTE.&Type({SupportedAttributes}{@type}),
    contextList         SET SIZE (1..MAX) OF Context,
    ...} OPTIONAL,
  ...
}

AttributeType ::= ATTRIBUTE.&id

AttributeValue ::= ATTRIBUTE.&Type

Context ::= SEQUENCE {
  contextType    CONTEXT.&id({SupportedContexts}),
  contextValues
    SET SIZE (1..MAX) OF CONTEXT.&Type({SupportedContexts}{@contextType}),
  fallback       BOOLEAN DEFAULT FALSE,
  ...
}

AttributeValueAssertion ::= SEQUENCE {
  type              ATTRIBUTE.&id({SupportedAttributes}),
  assertion
    ATTRIBUTE.&equality-match.&AssertionType
      ({SupportedAttributes}{@type}),
  assertedContexts
    CHOICE {allContexts       [0]  NULL,
            selectedContexts  [1]  SET SIZE (1..MAX) OF ContextAssertion
  } OPTIONAL,
  ...
}

ContextAssertion ::= SEQUENCE {
  contextType    CONTEXT.&id({SupportedContexts}),
  contextValues
```

```
    SET SIZE (1..MAX) OF
      CONTEXT.&Assertion({SupportedContexts}{@contextType}),
  ...
}

AttributeTypeAssertion ::= SEQUENCE {
  type              ATTRIBUTE.&id({SupportedAttributes}),
  assertedContexts  SEQUENCE SIZE (1..MAX) OF ContextAssertion OPTIONAL,
  ...
}

-- Definition of the following information object set is deferred, perhaps to
standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the values component of Attribute, the value component
-- of AttributeTypeAndValue, and the assertion component of AttributeValueAssertion.
SupportedAttributes ATTRIBUTE ::=
  {objectClass | aliasedEntryName, ...}

-- Definition of the following information object set is deferred, perhaps to
standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the context specifications
SupportedContexts CONTEXT ::=
  {...}

-- naming data types
Name ::= CHOICE { -- only one possibility for now --rdnSequence  RDNSequence
}

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

DistinguishedName ::= RDNSequence

RelativeDistinguishedName ::=
  SET SIZE (1..MAX) OF AttributeTypeAndDistinguishedValue

AttributeTypeAndDistinguishedValue ::= SEQUENCE {
  type                  ATTRIBUTE.&id({SupportedAttributes}),
  value                 ATTRIBUTE.&Type({SupportedAttributes}{@type}),
  primaryDistinguished  BOOLEAN DEFAULT TRUE,
  valuesWithContext
    SET SIZE (1..MAX) OF
      SEQUENCE {distingAttrValue
                  [0]  ATTRIBUTE.&Type({SupportedAttributes}{@type})
                    OPTIONAL,
                contextList       SET SIZE (1..MAX) OF Context,
                ...} OPTIONAL,
  ...
}

-- subtree data types
SubtreeSpecification ::= SEQUENCE {
  base                 [0]  LocalName DEFAULT {},
  COMPONENTS OF ChopSpecification,
  specificationFilter  [4]  Refinement OPTIONAL,
  ...
}

-- empty sequence specifies whole administrative area
LocalName ::= RDNSequence

ChopSpecification ::= SEQUENCE {
  specificExclusions
    [1]  SET SIZE (1..MAX) OF
           CHOICE {chopBefore  [0]  LocalName,
                   chopAfter   [1]  LocalName,
                   ...} OPTIONAL,
```

```
  minimum             [2]  BaseDistance DEFAULT 0,
  maximum             [3]  BaseDistance OPTIONAL,
  ...
}

BaseDistance ::= INTEGER(0..MAX)

Refinement ::= CHOICE {
  item  [0]  OBJECT-CLASS.&id,
  and   [1]  SET SIZE (1..MAX) OF Refinement,
  or    [2]  SET SIZE (1..MAX) OF Refinement,
  not   [3]  Refinement,
  ...
}

-- OBJECT-CLASS information object class specification
OBJECT-CLASS ::= CLASS {
  &Superclasses         OBJECT-CLASS OPTIONAL,
  &kind                 ObjectClassKind DEFAULT structural,
  &MandatoryAttributes  ATTRIBUTE OPTIONAL,
  &OptionalAttributes   ATTRIBUTE OPTIONAL,
  &id                   OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  [SUBCLASS OF &Superclasses]
  [KIND &kind]
  [MUST CONTAIN &MandatoryAttributes]
  [MAY CONTAIN &OptionalAttributes]
  ID &id
}

ObjectClassKind ::= ENUMERATED {abstract(0), structural(1), auxiliary(2)}

-- object classes
top OBJECT-CLASS ::= {
  KIND          abstract
  MUST CONTAIN  {objectClass}
  ID            id-oc-top
}

alias OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {aliasedEntryName}
  ID            id-oc-alias
}

parent OBJECT-CLASS ::= {KIND  abstract
                         ID    id-oc-parent
}

child OBJECT-CLASS ::= {KIND  auxiliary
                        ID    id-oc-child
}

-- ATTRIBUTE information object class specification
ATTRIBUTE ::= CLASS {
  &derivation             ATTRIBUTE OPTIONAL,
  &Type                   OPTIONAL, -- either &Type or &derivation required
  &equality-match         MATCHING-RULE OPTIONAL,
  &ordering-match         MATCHING-RULE OPTIONAL,
  &substrings-match       MATCHING-RULE OPTIONAL,
  &single-valued          BOOLEAN DEFAULT FALSE,
  &collective             BOOLEAN DEFAULT FALSE,
  &dummy                  BOOLEAN DEFAULT FALSE,
  -- operational extensions
  &no-user-modification   BOOLEAN DEFAULT FALSE,
  &usage                  AttributeUsage DEFAULT userApplications,
  &id                     OBJECT IDENTIFIER UNIQUE
```

```
}
WITH SYNTAX {
  [SUBTYPE OF &derivation]
  [WITH SYNTAX &Type]
  [EQUALITY MATCHING RULE &equality-match]
  [ORDERING MATCHING RULE &ordering-match]
  [SUBSTRINGS MATCHING RULE &substrings-match]
  [SINGLE VALUE &single-valued]
  [COLLECTIVE &collective]
  [DUMMY &dummy]
  [NO USER MODIFICATION &no-user-modification]
  [USAGE &usage]
  ID &id
}

AttributeUsage ::= ENUMERATED {
  userApplications(0), directoryOperation(1), distributedOperation(2),
  dSAOperation(3),...}

-- attributes
objectClass ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-at-objectClass
}

aliasedEntryName ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  ID                      id-at-aliasedEntryName
}

-- MATCHING-RULE information object class specification
MATCHING-RULE ::= CLASS {
  &ParentMatchingRules   MATCHING-RULE OPTIONAL,
  &AssertionType         OPTIONAL,
  &uniqueMatchIndicator  ATTRIBUTE OPTIONAL,
  &id                    OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  [PARENT &ParentMatchingRules]
  [SYNTAX &AssertionType]
  [UNIQUE-MATCH-INDICATOR &uniqueMatchIndicator]
  ID &id
}

-- matching rules
objectIdentifierMatch MATCHING-RULE ::= {
  SYNTAX  OBJECT IDENTIFIER
  ID      id-mr-objectIdentifierMatch
}

distinguishedNameMatch MATCHING-RULE ::= {
  SYNTAX  DistinguishedName
  ID      id-mr-distinguishedNameMatch
}

MAPPING-BASED-MATCHING{SelectedBy, BOOLEAN:combinable, MappingResult,
                       OBJECT IDENTIFIER:matchingRule} ::= CLASS {
  &selectBy          SelectedBy OPTIONAL,
  &ApplicableTo      ATTRIBUTE,
  &subtypesIncluded  BOOLEAN DEFAULT TRUE,
  &combinable        BOOLEAN(combinable),
  &mappingResults    MappingResult OPTIONAL,
  &userControl       BOOLEAN DEFAULT FALSE,
  &exclusive         BOOLEAN DEFAULT TRUE,
  &matching-rule     MATCHING-RULE.&id(matchingRule),
```

```
  &id                OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  [SELECT BY &selectBy]
  APPLICABLE TO &ApplicableTo
  [SUBTYPES INCLUDED &subtypesIncluded]
  COMBINABLE &combinable
  [MAPPING RESULTS &mappingResults]
  [USER CONTROL &userControl]
  [EXCLUSIVE &exclusive]
  MATCHING RULE &matching-rule
  ID &id
}

-- NAME-FORM information object class specification
NAME-FORM ::= CLASS {
  &namedObjectClass     OBJECT-CLASS,
  &MandatoryAttributes  ATTRIBUTE,
  &OptionalAttributes   ATTRIBUTE OPTIONAL,
  &id                   OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  NAMES &namedObjectClass
  WITH ATTRIBUTES &MandatoryAttributes
  [AND OPTIONALLY &OptionalAttributes]
  ID &id
}

-- STRUCTURE-RULE class and DIT structure rule data types
DITStructureRule ::= SEQUENCE {
  ruleIdentifier          RuleIdentifier,
  -- shall be unique within the scope of the subschema
  nameForm                NAME-FORM.&id,
  superiorStructureRules  SET SIZE (1..MAX) OF RuleIdentifier OPTIONAL,
  ...
}

RuleIdentifier ::= INTEGER

STRUCTURE-RULE ::= CLASS {
  &nameForm                NAME-FORM,
  &SuperiorStructureRules  STRUCTURE-RULE OPTIONAL,
  &id                      RuleIdentifier
}
WITH SYNTAX {
  NAME FORM &nameForm
  [SUPERIOR RULES &SuperiorStructureRules]
  ID &id
}

-- DIT content rule data type and CONTENT-RULE class
DITContentRule ::= SEQUENCE {
  structuralObjectClass  OBJECT-CLASS.&id,
  auxiliaries            SET SIZE (1..MAX) OF OBJECT-CLASS.&id OPTIONAL,
  mandatory              [1]  SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  optional               [2]  SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  precluded              [3]  SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  ...
}

CONTENT-RULE ::= CLASS {
  &structuralClass  OBJECT-CLASS.&id UNIQUE,
  &Auxiliaries      OBJECT-CLASS OPTIONAL,
  &Mandatory        ATTRIBUTE OPTIONAL,
  &Optional         ATTRIBUTE OPTIONAL,
  &Precluded        ATTRIBUTE OPTIONAL
}
WITH SYNTAX {
```

```
  STRUCTURAL OBJECT-CLASS &structuralClass
  [AUXILIARY OBJECT-CLASSES &Auxiliaries]
  [MUST CONTAIN &Mandatory]
  [MAY CONTAIN &Optional]
  [MUST-NOT CONTAIN &Precluded]
}

CONTEXT ::= CLASS {
  &Type          ,
  &DefaultValue  OPTIONAL,
  &Assertion     OPTIONAL,
  &absentMatch   BOOLEAN DEFAULT TRUE,
  &id            OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  WITH SYNTAX &Type
  [DEFAULT-VALUE &DefaultValue]
  [ASSERTED AS &Assertion]
  [ABSENT-MATCH &absentMatch]
  ID &id
}

DITContextUse ::= SEQUENCE {
  attributeType      ATTRIBUTE.&id,
  mandatoryContexts  [1]  SET SIZE (1..MAX) OF CONTEXT.&id OPTIONAL,
  optionalContexts   [2]  SET SIZE (1..MAX) OF CONTEXT.&id OPTIONAL,
  ...
}

DIT-CONTEXT-USE-RULE ::= CLASS {
  &attributeType  ATTRIBUTE.&id UNIQUE,
  &Mandatory      CONTEXT OPTIONAL,
  &Optional       CONTEXT OPTIONAL
}
WITH SYNTAX {
  ATTRIBUTE TYPE &attributeType
  [MANDATORY CONTEXTS &Mandatory]
  [OPTIONAL CONTEXTS &Optional]
}

FRIENDS ::= CLASS {
  &anchor   ATTRIBUTE.&id UNIQUE,
  &Friends  ATTRIBUTE
}WITH SYNTAX {ANCHOR &anchor
              FRIENDS &Friends
}

-- system schema information objects
-- object classes
subentry OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          structural
  MUST CONTAIN  {commonName | subtreeSpecification}
  ID            id-sc-subentry
}

subentryNameForm NAME-FORM ::= {
  NAMES            subentry
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-subentryNameForm
}

subtreeSpecification ATTRIBUTE ::= {
  WITH SYNTAX  SubtreeSpecification
  USAGE        directoryOperation
  ID           id-oa-subtreeSpecification
}
```

```
administrativeRole ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT-CLASS.&id
  EQUALITY MATCHING RULE  objectIdentifierMatch
  USAGE                   directoryOperation
  ID                      id-oa-administrativeRole
}

createTimestamp ATTRIBUTE ::= {
  WITH SYNTAX             GeneralizedTime
  -- as per 46.3 b) or c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
  EQUALITY MATCHING RULE  generalizedTimeMatch
  ORDERING MATCHING RULE  generalizedTimeOrderingMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-createTimestamp
}

modifyTimestamp ATTRIBUTE ::= {
  WITH SYNTAX             GeneralizedTime
  -- as per 46.3 b) or c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
  EQUALITY MATCHING RULE  generalizedTimeMatch
  ORDERING MATCHING RULE  generalizedTimeOrderingMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-modifyTimestamp
}

subschemaTimestamp ATTRIBUTE ::= {
  WITH SYNTAX             GeneralizedTime
  -- as per 46.3 b) or c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
  EQUALITY MATCHING RULE  generalizedTimeMatch
  ORDERING MATCHING RULE  generalizedTimeOrderingMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-subschemaTimestamp
}

creatorsName ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-creatorsName
}

modifiersName ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-modifiersName
}

subschemaSubentryList ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-subschemaSubentryList
}

accessControlSubentryList ATTRIBUTE ::= {
```

```
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-accessControlSubentryList
}

collectiveAttributeSubentryList ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-collectiveAttributeSubentryList
}

contextDefaultSubentryList ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-contextDefaultSubentryList
}

serviceAdminSubentryList ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-serviceAdminSubentryList
}

hasSubordinates ATTRIBUTE ::= {
  WITH SYNTAX             BOOLEAN
  EQUALITY MATCHING RULE  booleanMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-hasSubordinates
}

accessControlSubentry OBJECT-CLASS ::= {
  KIND  auxiliary
  ID    id-sc-accessControlSubentry
}

collectiveAttributeSubentry OBJECT-CLASS ::= {
  KIND  auxiliary
  ID    id-sc-collectiveAttributeSubentry
}

collectiveExclusions ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  USAGE                   directoryOperation
  ID                      id-oa-collectiveExclusions
}

contextAssertionSubentry OBJECT-CLASS ::= {
  KIND          auxiliary
  MUST CONTAIN  {contextAssertionDefaults}
  ID            id-sc-contextAssertionSubentry
}

contextAssertionDefaults ATTRIBUTE ::= {
  WITH SYNTAX             TypeAndContextAssertion
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-oa-contextAssertionDefault
```

```
}

serviceAdminSubentry OBJECT-CLASS ::= {
  KIND          auxiliary
  MUST CONTAIN  {searchRules}
  ID            id-sc-serviceAdminSubentry
}

searchRules ATTRIBUTE ::= {
  WITH SYNTAX             SearchRuleDescription
  EQUALITY MATCHING RULE  integerFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-oa-searchRules
}

SearchRuleDescription ::= SEQUENCE {
  COMPONENTS OF SearchRule,
  name         [28]  SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  [29]  UnboundedDirectoryString OPTIONAL,
  ...
}

hierarchyLevel ATTRIBUTE ::= {
  WITH SYNTAX             HierarchyLevel
  EQUALITY MATCHING RULE  integerMatch
  ORDERING MATCHING RULE  integerOrderingMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-hierarchyLevel
}

HierarchyLevel ::= INTEGER

hierarchyBelow ATTRIBUTE ::= {
  WITH SYNTAX             HierarchyBelow
  EQUALITY MATCHING RULE  booleanMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-oa-hierarchyBelow
}

HierarchyBelow ::= BOOLEAN

hierarchyParent ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  USAGE                   directoryOperation
  ID                      id-oa-hierarchyParent
}

hierarchyTop ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  SINGLE VALUE            TRUE
  USAGE                   directoryOperation
  ID                      id-oa-hierarchyTop
}

-- object identifier assignments
-- object classes
id-oc-top OBJECT IDENTIFIER ::=
  {id-oc 0}

id-oc-alias OBJECT IDENTIFIER ::= {id-oc 1}
```

```
id-oc-parent OBJECT IDENTIFIER ::= {id-oc 28}

id-oc-child OBJECT IDENTIFIER ::= {id-oc 29}

-- attributes
id-at-objectClass OBJECT IDENTIFIER ::= {id-at 0}

id-at-aliasedEntryName OBJECT IDENTIFIER ::= {id-at 1}

-- matching rules
id-mr-objectIdentifierMatch OBJECT IDENTIFIER ::= {id-mr 0}

id-mr-distinguishedNameMatch OBJECT IDENTIFIER ::= {id-mr 1}

-- operational attributes
id-oa-excludeAllCollectiveAttributes OBJECT IDENTIFIER ::=
  {id-oa 0}

id-oa-createTimestamp OBJECT IDENTIFIER ::= {id-oa 1}

id-oa-modifyTimestamp OBJECT IDENTIFIER ::= {id-oa 2}

id-oa-creatorsName OBJECT IDENTIFIER ::= {id-oa 3}

id-oa-modifiersName OBJECT IDENTIFIER ::= {id-oa 4}

id-oa-administrativeRole OBJECT IDENTIFIER ::= {id-oa 5}

id-oa-subtreeSpecification OBJECT IDENTIFIER ::= {id-oa 6}

id-oa-collectiveExclusions OBJECT IDENTIFIER ::= {id-oa 7}

id-oa-subschemaTimestamp OBJECT IDENTIFIER ::= {id-oa 8}

id-oa-hasSubordinates OBJECT IDENTIFIER ::= {id-oa 9}

id-oa-subschemaSubentryList OBJECT IDENTIFIER ::= {id-oa 10}

id-oa-accessControlSubentryList OBJECT IDENTIFIER ::= {id-oa 11}

id-oa-collectiveAttributeSubentryList OBJECT IDENTIFIER ::= {id-oa 12}

id-oa-contextDefaultSubentryList OBJECT IDENTIFIER ::= {id-oa 13}

id-oa-contextAssertionDefault OBJECT IDENTIFIER ::= {id-oa 14}

id-oa-serviceAdminSubentryList OBJECT IDENTIFIER ::= {id-oa 15}

id-oa-searchRules OBJECT IDENTIFIER ::= {id-oa 16}

id-oa-hierarchyLevel OBJECT IDENTIFIER ::= {id-oa 17}

id-oa-hierarchyBelow OBJECT IDENTIFIER ::= {id-oa 18}

id-oa-hierarchyParent OBJECT IDENTIFIER ::= {id-oa 19}

id-oa-hierarchyTop OBJECT IDENTIFIER ::= {id-oa 20}

-- subentry classes
id-sc-subentry OBJECT IDENTIFIER ::= {id-sc 0}

id-sc-accessControlSubentry OBJECT IDENTIFIER ::= {id-sc 1}

id-sc-collectiveAttributeSubentry OBJECT IDENTIFIER ::= {id-sc 2}

id-sc-contextAssertionSubentry OBJECT IDENTIFIER ::= {id-sc 3}

id-sc-serviceAdminSubentry OBJECT IDENTIFIER ::= {id-sc 4}
```

```
--  Name forms
id-nf-subentryNameForm OBJECT IDENTIFIER ::= {id-nf 16}

-- administrative roles
id-ar-autonomousArea OBJECT IDENTIFIER ::= {id-ar 1}

id-ar-accessControlSpecificArea OBJECT IDENTIFIER ::= {id-ar 2}

id-ar-accessControlInnerArea OBJECT IDENTIFIER ::= {id-ar 3}

id-ar-subschemaAdminSpecificArea OBJECT IDENTIFIER ::= {id-ar 4}

id-ar-collectiveAttributeSpecificArea OBJECT IDENTIFIER ::= {id-ar 5}

id-ar-collectiveAttributeInnerArea OBJECT IDENTIFIER ::= {id-ar 6}

id-ar-contextDefaultSpecificArea OBJECT IDENTIFIER ::= {id-ar 7}

id-ar-serviceSpecificArea OBJECT IDENTIFIER ::= {id-ar 8}

END -- InformationFramework
```

Annex C

SubSchema Administration Schema in ASN.1

Replace the ASN.1 module in Annex C with the following

```
SchemaAdministration {joint-iso-itu-t ds(5) module(1) schemaAdministration(23)
  6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  id-soa, id-soc, informationFramework, selectedAttributeTypes
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  ATTRIBUTE, AttributeUsage, CONTEXT, DITContentRule, DITStructureRule,
    MATCHING-RULE, NAME-FORM, OBJECT-CLASS, ObjectClassKind,
    objectIdentifierMatch
    FROM InformationFramework informationFramework
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  integerFirstComponentMatch, integerMatch,
    objectIdentifierFirstComponentMatch, UnboundedDirectoryString
    FROM SelectedAttributeTypes selectedAttributeTypes;

subschema OBJECT-CLASS ::= {
  KIND         auxiliary
  MAY CONTAIN
    {dITStructureRules | nameForms | dITContentRules | objectClasses |
      attributeTypes | friends | contextTypes | dITContextUse | matchingRules |
      matchingRuleUse}
  ID           id-soc-subschema
}
```

```
dITStructureRules ATTRIBUTE ::= {
  WITH SYNTAX             DITStructureRuleDescription
  EQUALITY MATCHING RULE  integerFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-dITStructureRule
}

DITStructureRuleDescription ::= SEQUENCE {
  COMPONENTS OF DITStructureRule,
  name         [1]  SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  ...
}

dITContentRules ATTRIBUTE ::= {
  WITH SYNTAX             DITContentRuleDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-dITContentRules
}

DITContentRuleDescription ::= SEQUENCE {
  COMPONENTS OF DITContentRule,
  name         [4]  SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  ...
}

matchingRules ATTRIBUTE ::= {
  WITH SYNTAX             MatchingRuleDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-matchingRules
}

MatchingRuleDescription ::= SEQUENCE {
  identifier   MATCHING-RULE.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  UnboundedDirectoryString OPTIONAL,
  ...
}

-- describes the ASN.1 syntax
attributeTypes ATTRIBUTE ::= {
  WITH SYNTAX             AttributeTypeDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-attributeTypes
}

AttributeTypeDescription ::= SEQUENCE {
  identifier   ATTRIBUTE.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  AttributeTypeInformation,
  ...
}

AttributeTypeInformation ::= SEQUENCE {
  derivation       [0]  ATTRIBUTE.&id OPTIONAL,
  equalityMatch    [1]  MATCHING-RULE.&id OPTIONAL,
  orderingMatch    [2]  MATCHING-RULE.&id OPTIONAL,
  substringsMatch  [3]  MATCHING-RULE.&id OPTIONAL,
```

```
  attributeSyntax  [4]  UnboundedDirectoryString OPTIONAL,
  multi-valued     [5]  BOOLEAN DEFAULT TRUE,
  collective       [6]  BOOLEAN DEFAULT FALSE,
  userModifiable   [7]  BOOLEAN DEFAULT TRUE,
  application      AttributeUsage DEFAULT userApplications,
  ...
}

objectClasses ATTRIBUTE ::= {
  WITH SYNTAX             ObjectClassDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-objectClasses
}

ObjectClassDescription ::= SEQUENCE {
  identifier   OBJECT-CLASS.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  ObjectClassInformation,
  ...
}

ObjectClassInformation ::= SEQUENCE {
  subclassOf   SET SIZE (1..MAX) OF OBJECT-CLASS.&id OPTIONAL,
  kind         ObjectClassKind DEFAULT structural,
  mandatories  [3]  SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  optionals    [4]  SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  ...
}

nameForms ATTRIBUTE ::= {
  WITH SYNTAX             NameFormDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-nameForms
}

NameFormDescription ::= SEQUENCE {
  identifier   NAME-FORM.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  NameFormInformation,
  ...
}

NameFormInformation ::= SEQUENCE {
  subordinate        OBJECT-CLASS.&id,
  namingMandatories  SET OF ATTRIBUTE.&id,
  namingOptionals    SET SIZE (1..MAX) OF ATTRIBUTE.&id OPTIONAL,
  ...
}

matchingRuleUse ATTRIBUTE ::= {
  WITH SYNTAX             MatchingRuleUseDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-matchingRuleUse
}

MatchingRuleUseDescription ::= SEQUENCE {
  identifier   MATCHING-RULE.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  SET OF ATTRIBUTE.&id,
```

```
  ...
}

structuralObjectClass ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-soa-structuralObjectClass
}

governingStructureRule ATTRIBUTE ::= {
  WITH SYNTAX             INTEGER
  EQUALITY MATCHING RULE  integerMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   directoryOperation
  ID                      id-soa-governingStructureRule
}

contextTypes ATTRIBUTE ::= {
  WITH SYNTAX             ContextDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-contextTypes
}

ContextDescription ::= SEQUENCE {
  identifier   CONTEXT.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  ContextInformation,
  ...
}

ContextInformation ::= SEQUENCE {
  syntax           UnboundedDirectoryString,
  assertionSyntax  UnboundedDirectoryString OPTIONAL,
  ...
}

dITContextUse ATTRIBUTE ::= {
  WITH SYNTAX             DITContextUseDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-soa-dITContextUse
}

DITContextUseDescription ::= SEQUENCE {
  identifier   ATTRIBUTE.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  information  [0]  DITContextUseInformation,
  ...
}

DITContextUseInformation ::= SEQUENCE {
  mandatoryContexts  [1]  SET SIZE (1..MAX) OF CONTEXT.&id OPTIONAL,
  optionalContexts   [2]  SET SIZE (1..MAX) OF CONTEXT.&id OPTIONAL,
  ...
}

friends ATTRIBUTE ::= {
  WITH SYNTAX             FriendsDescription
  EQUALITY MATCHING RULE  objectIdentifierFirstComponentMatch
```

```
  USAGE                   directoryOperation
  ID                      id-soa-friends
}

FriendsDescription ::= SEQUENCE {
  anchor       ATTRIBUTE.&id,
  name         SET SIZE (1..MAX) OF UnboundedDirectoryString OPTIONAL,
  description  UnboundedDirectoryString OPTIONAL,
  obsolete     BOOLEAN DEFAULT FALSE,
  friends      [0]  SET SIZE (1..MAX) OF ATTRIBUTE.&id,
  ...
}

-- object identifier assignments
-- schema object classes
id-soc-subschema OBJECT IDENTIFIER ::=
  {id-soc 1}

-- schema operational attributes
id-soa-dITStructureRule OBJECT IDENTIFIER ::=
  {id-soa 1}

id-soa-dITContentRules OBJECT IDENTIFIER ::= {id-soa 2}

id-soa-matchingRules OBJECT IDENTIFIER ::= {id-soa 4}

id-soa-attributeTypes OBJECT IDENTIFIER ::= {id-soa 5}

id-soa-objectClasses OBJECT IDENTIFIER ::= {id-soa 6}

id-soa-nameForms OBJECT IDENTIFIER ::= {id-soa 7}

id-soa-matchingRuleUse OBJECT IDENTIFIER ::= {id-soa 8}

id-soa-structuralObjectClass OBJECT IDENTIFIER ::= {id-soa 9}

id-soa-governingStructureRule OBJECT IDENTIFIER ::= {id-soa 10}

id-soa-contextTypes OBJECT IDENTIFIER ::= {id-soa 11}

id-soa-dITContextUse OBJECT IDENTIFIER ::= {id-soa 12}

id-soa-friends OBJECT IDENTIFIER ::= {id-soa 13}

END -- SchemaAdministration
```

Annex D

Service Administration in ASN.1

Replace the ASN.1 module in Annex D with the following

```
ServiceAdministration {joint-iso-itu-t ds(5) module(1)
  serviceAdministration(33) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
```

```
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryAbstractService, informationFramework
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  ATTRIBUTE, AttributeType, CONTEXT, MATCHING-RULE, OBJECT-CLASS,
    SupportedAttributes, SupportedContexts
    FROM InformationFramework informationFramework
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  FamilyGrouping, FamilyReturn, HierarchySelections, SearchControlOptions,
    ServiceControlOptions
    FROM DirectoryAbstractService directoryAbstractService;

-- types
SearchRule ::= SEQUENCE {
  COMPONENTS OF SearchRuleId,
  serviceType           [1]  OBJECT IDENTIFIER OPTIONAL,
  userClass             [2]  INTEGER OPTIONAL,
  inputAttributeTypes
    [3]  SEQUENCE SIZE (0..MAX) OF RequestAttribute OPTIONAL,
  attributeCombination  [4]  AttributeCombination DEFAULT and:{},
  outputAttributeTypes  [5]  SEQUENCE SIZE (1..MAX) OF ResultAttribute OPTIONAL,
  defaultControls       [6]  ControlOptions OPTIONAL,
  mandatoryControls     [7]  ControlOptions OPTIONAL,
  searchRuleControls    [8]  ControlOptions OPTIONAL,
  familyGrouping        [9]  FamilyGrouping OPTIONAL,
  familyReturn          [10]  FamilyReturn OPTIONAL,
  relaxation            [11]  RelaxationPolicy OPTIONAL,
  additionalControl     [12]  SEQUENCE SIZE (1..MAX) OF AttributeType OPTIONAL,
  allowedSubset         [13]  AllowedSubset DEFAULT '111'B,
  imposedSubset         [14]  ImposedSubset OPTIONAL,
  entryLimit            [15]  EntryLimit OPTIONAL,
  ...
}

SearchRuleId ::= SEQUENCE {id     INTEGER,
                           dmdId  [0]  OBJECT IDENTIFIER
}

AllowedSubset ::= BIT STRING {baseObject(0), oneLevel(1), wholeSubtree(2)}

ImposedSubset ::= ENUMERATED {baseObject(0), oneLevel(1), wholeSubtree(2),...}

RequestAttribute ::= SEQUENCE {
  attributeType       ATTRIBUTE.&id({SupportedAttributes}),
  includeSubtypes     [0]  BOOLEAN DEFAULT FALSE,
  selectedValues
    [1]  SEQUENCE SIZE (0..MAX) OF
           ATTRIBUTE.&Type({SupportedAttributes}{@attributeType}) OPTIONAL,
  defaultValues
    [2]  SEQUENCE SIZE (0..MAX) OF
           SEQUENCE {entryType  OBJECT-CLASS.&id OPTIONAL,
                     values
                       SEQUENCE OF
                         ATTRIBUTE.&Type
                           ({SupportedAttributes}{@attributeType}),
                     ...} OPTIONAL,
  contexts            [3]  SEQUENCE SIZE (0..MAX) OF ContextProfile OPTIONAL,
  contextCombination  [4]  ContextCombination DEFAULT and:{},
  matchingUse         [5]  SEQUENCE SIZE (1..MAX) OF MatchingUse OPTIONAL,
  ...
}

ContextProfile ::= SEQUENCE {
  contextType   CONTEXT.&id({SupportedContexts}),
  contextValue
    SEQUENCE SIZE (1..MAX) OF
      CONTEXT.&Assertion({SupportedContexts}{@contextType}) OPTIONAL,
```

```
  ...
}

ContextCombination ::= CHOICE {
  context  [0]  CONTEXT.&id({SupportedContexts}),
  and      [1]  SEQUENCE OF ContextCombination,
  or       [2]  SEQUENCE OF ContextCombination,
  not      [3]  ContextCombination,
  ...
}

MatchingUse ::= SEQUENCE {
  restrictionType
    MATCHING-RESTRICTION.&id({SupportedMatchingRestrictions}),
  restrictionValue
    MATCHING-RESTRICTION.&Restriction
      ({SupportedMatchingRestrictions}{@restrictionType}),
  ...
}

-- Definition of the following information object set is deferred, perhaps to
standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the components of SupportedMatchingRestrictions
SupportedMatchingRestrictions MATCHING-RESTRICTION ::=
  {...}

AttributeCombination ::= CHOICE {
  attribute  [0]  AttributeType,
  and        [1]  SEQUENCE OF AttributeCombination,
  or         [2]  SEQUENCE OF AttributeCombination,
  not        [3]  AttributeCombination,
  ...
}

ResultAttribute ::= SEQUENCE {
  attributeType  ATTRIBUTE.&id({SupportedAttributes}),
  outputValues
    CHOICE {selectedValues
              SEQUENCE OF
                ATTRIBUTE.&Type({SupportedAttributes}{@attributeType}),
            matchedValuesOnly  NULL} OPTIONAL,
  contexts       [0]  SEQUENCE SIZE (1..MAX) OF ContextProfile OPTIONAL,
  ...
}

ControlOptions ::= SEQUENCE {
  serviceControls   [0]  ServiceControlOptions DEFAULT {},
  searchOptions     [1]  SearchControlOptions DEFAULT {searchAliases},
  hierarchyOptions  [2]  HierarchySelections OPTIONAL,
  ...
}

EntryLimit ::= SEQUENCE {default  INTEGER,
                         max      INTEGER,
                         ...
}

RelaxationPolicy ::= SEQUENCE {
  basic        [0]  MRMapping DEFAULT {},
  tightenings  [1]  SEQUENCE SIZE (1..MAX) OF MRMapping OPTIONAL,
  relaxations  [2]  SEQUENCE SIZE (1..MAX) OF MRMapping OPTIONAL,
  maximum      [3]  INTEGER OPTIONAL, -- mandatory if tightenings is present
  minimum      [4]  INTEGER DEFAULT 1,
  ...
}

MRMapping ::= SEQUENCE {
```

```
  mapping       [0]  SEQUENCE SIZE (1..MAX) OF Mapping OPTIONAL,
  substitution  [1]  SEQUENCE SIZE (1..MAX) OF MRSubstitution OPTIONAL,
  ...
}

Mapping ::= SEQUENCE {
  mappingFunction
    OBJECT IDENTIFIER
      (CONSTRAINED BY {-- shall be an--

         -- object identifier of a mapping-based matching algorithm -- }),
  level            INTEGER DEFAULT 0,
  ...
}

MRSubstitution ::= SEQUENCE {
  attribute        AttributeType,
  oldMatchingRule  [0]  MATCHING-RULE.&id OPTIONAL,
  newMatchingRule  [1]  MATCHING-RULE.&id OPTIONAL,
  ...
}

-- ASN.1 information object classes
SEARCH-RULE ::= CLASS {
  &dmdId                 OBJECT IDENTIFIER,
  &serviceType           OBJECT IDENTIFIER OPTIONAL,
  &userClass             INTEGER OPTIONAL,
  &InputAttributeTypes   REQUEST-ATTRIBUTE OPTIONAL,
  &combination           AttributeCombination OPTIONAL,
  &OutputAttributeTypes  RESULT-ATTRIBUTE OPTIONAL,
  &defaultControls       ControlOptions OPTIONAL,
  &mandatoryControls     ControlOptions OPTIONAL,
  &searchRuleControls    ControlOptions OPTIONAL,
  &familyGrouping        FamilyGrouping OPTIONAL,
  &familyReturn          FamilyReturn OPTIONAL,
  &additionalControl     AttributeType OPTIONAL,
  &relaxation            RelaxationPolicy OPTIONAL,
  &allowedSubset         AllowedSubset DEFAULT '111'B,
  &imposedSubset         ImposedSubset OPTIONAL,
  &entryLimit            EntryLimit OPTIONAL,
  &id                    INTEGER UNIQUE
}
WITH SYNTAX {
  DMD ID &dmdId
  [SERVICE-TYPE &serviceType]
  [USER-CLASS &userClass]
  [INPUT ATTRIBUTES &InputAttributeTypes]
  [COMBINATION &combination]
  [OUTPUT ATTRIBUTES &OutputAttributeTypes]
  [DEFAULT CONTROL &defaultControls]
  [MANDATORY CONTROL &mandatoryControls]
  [SEARCH-RULE CONTROL &searchRuleControls]
  [FAMILY-GROUPING &familyGrouping]
  [FAMILY-RETURN &familyReturn]
  [ADDITIONAL CONTROL &additionalControl]
  [RELAXATION &relaxation]
  [ALLOWED SUBSET &allowedSubset]
  [IMPOSED SUBSET &imposedSubset]
  [ENTRY LIMIT &entryLimit]
  ID &id
}

REQUEST-ATTRIBUTE ::= CLASS {
  &attributeType       ATTRIBUTE.&id,
  &SelectedValues      ATTRIBUTE.&Type OPTIONAL,
  &DefaultValues       SEQUENCE {entryType  OBJECT-CLASS.&id OPTIONAL,
                                 values     SEQUENCE OF ATTRIBUTE.&Type
  } OPTIONAL,
```

```
  &contexts            SEQUENCE OF ContextProfile OPTIONAL,
  &contextCombination  ContextCombination OPTIONAL,
  &MatchingUse         MatchingUse OPTIONAL,
  &includeSubtypes     BOOLEAN DEFAULT FALSE
}
WITH SYNTAX {
  ATTRIBUTE TYPE &attributeType
  [SELECTED VALUES &SelectedValues]
  [DEFAULT VALUES &DefaultValues]
  [CONTEXTS &contexts]
  [CONTEXT COMBINATION &contextCombination]
  [MATCHING USE &MatchingUse]
  [INCLUDE SUBTYPES &includeSubtypes]
}

RESULT-ATTRIBUTE ::= CLASS {
  &attributeType  ATTRIBUTE.&id,
  &outputValues   CHOICE {selectedValues
                             SEQUENCE OF ATTRIBUTE.&Type,
                          matchedValuesOnly  NULL
  } OPTIONAL,
  &contexts       ContextProfile OPTIONAL
}
WITH SYNTAX {
  ATTRIBUTE TYPE &attributeType
  [OUTPUT VALUES &outputValues]
  [CONTEXTS &contexts]
}

MATCHING-RESTRICTION ::= CLASS {
  &Restriction  ,
  &Rules        MATCHING-RULE.&id,
  &id           OBJECT IDENTIFIER UNIQUE
}WITH SYNTAX {RESTRICTION &Restriction
              RULES &Rules
              ID &id
}

END -- ServiceAdministration
```

Annex E

Basic Access Control in ASN.1

Replace the ASN.1 module in Annex E with the following

```
BasicAccessControl {joint-iso-itu-t ds(5) module(1) basicAccessControl(24) 6}
DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryAbstractService, id-aca, id-acScheme, informationFramework,
    selectedAttributeTypes
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
```

```
  ATTRIBUTE, AttributeType, ContextAssertion, DistinguishedName, MATCHING-RULE,
    objectIdentifierMatch, Refinement, SubtreeSpecification,
    SupportedAttributes
    FROM InformationFramework informationFramework
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  Filter
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  directoryStringFirstComponentMatch, NameAndOptionalUID,
    UnboundedDirectoryString, UniqueIdentifier
    FROM SelectedAttributeTypes selectedAttributeTypes;

accessControlScheme ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  USAGE                   directoryOperation
  ID                      id-aca-accessControlScheme
}

-- types
ACIItem ::= SEQUENCE {
  identificationTag    UnboundedDirectoryString,
  precedence           Precedence,
  authenticationLevel  AuthenticationLevel,
  itemOrUserFirst
    CHOICE {itemFirst
              [0]  SEQUENCE {protectedItems   ProtectedItems,
                             itemPermissions  SET OF ItemPermission,
                             ...},
            userFirst
              [1]  SEQUENCE {userClasses      UserClasses,
                             userPermissions  SET OF UserPermission,
                             ...},
            ...},
...
}

Precedence ::= INTEGER(0..255,...)

ProtectedItems ::= SEQUENCE {
  entry                           [0]  NULL OPTIONAL,
  allUserAttributeTypes           [1]  NULL OPTIONAL,
  attributeType
    [2]  SET SIZE (1..MAX) OF AttributeType OPTIONAL,
  allAttributeValues
    [3]  SET SIZE (1..MAX) OF AttributeType OPTIONAL,
  allUserAttributeTypesAndValues  [4]  NULL OPTIONAL,
  attributeValue
    [5]  SET SIZE (1..MAX) OF AttributeTypeAndValue OPTIONAL,
  selfValue
    [6]  SET SIZE (1..MAX) OF AttributeType OPTIONAL,
  rangeOfValues                   [7]  Filter OPTIONAL,
  maxValueCount
    [8]  SET SIZE (1..MAX) OF MaxValueCount OPTIONAL,
  maxImmSub                       [9]  INTEGER OPTIONAL,
  restrictedBy
    [10]  SET SIZE (1..MAX) OF RestrictedValue OPTIONAL,
  contexts
    [11]  SET SIZE (1..MAX) OF ContextAssertion OPTIONAL,
  classes                         [12]  Refinement OPTIONAL,
  ...
}

MaxValueCount ::= SEQUENCE {type      AttributeType,
                            maxCount  INTEGER,
                            ...
}
```

```
RestrictedValue ::= SEQUENCE {type      AttributeType,
                              valuesIn  AttributeType,
                              ...
}

UserClasses ::= SEQUENCE {
  allUsers   [0]  NULL OPTIONAL,
  thisEntry  [1]  NULL OPTIONAL,
  name       [2]  SET SIZE (1..MAX) OF NameAndOptionalUID OPTIONAL,
  userGroup  [3]  SET SIZE (1..MAX) OF NameAndOptionalUID OPTIONAL,
  -- dn component shall be the name of an
  -- entry of GroupOfUniqueNames
  subtree    [4]  SET SIZE (1..MAX) OF SubtreeSpecification OPTIONAL,
  ...
}

ItemPermission ::= SEQUENCE {
  precedence        Precedence OPTIONAL,
  -- defaults to precedence in ACIItem
  userClasses       UserClasses,
  grantsAndDenials  GrantsAndDenials,
  ...
}

UserPermission ::= SEQUENCE {
  precedence        Precedence OPTIONAL,
  -- defaults to precedence in ACIItem
  protectedItems    ProtectedItems,
  grantsAndDenials  GrantsAndDenials,
  ...
}

AuthenticationLevel ::= CHOICE {
  basicLevels
    SEQUENCE {level           ENUMERATED {none(0), simple(1), strong(2),...},
              localQualifier  INTEGER OPTIONAL,
              signed          BOOLEAN DEFAULT FALSE,
              ...},
  other        EXTERNAL,
  ...
}

GrantsAndDenials ::= BIT STRING {
  -- permissions that may be used in conjunction
  -- with any component of ProtectedItems
  grantAdd(0), denyAdd(1), grantDiscloseOnError(2), denyDiscloseOnError(3),
  grantRead(4), denyRead(5), grantRemove(6),
  denyRemove(7),
  -- permissions that may be used only in conjunction
  -- with the entry component
  grantBrowse(8), denyBrowse(9), grantExport(10), denyExport(11),
  grantImport(12), denyImport(13), grantModify(14), denyModify(15),
  grantRename(16), denyRename(17), grantReturnDN(18),
  denyReturnDN(19),
  -- permissions that may be used in conjunction
  -- with any component, except entry, of ProtectedItems
  grantCompare(20), denyCompare(21), grantFilterMatch(22), denyFilterMatch(23),
  grantInvoke(24), denyInvoke(25)}

AttributeTypeAndValue ::= SEQUENCE {
  type   ATTRIBUTE.&id({SupportedAttributes}),
  value  ATTRIBUTE.&Type({SupportedAttributes}{@type}),
  ...
}

-- attributes
prescriptiveACI ATTRIBUTE ::= {
```

```
  WITH SYNTAX             ACIItem
  EQUALITY MATCHING RULE  directoryStringFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-aca-prescriptiveACI
}

entryACI ATTRIBUTE ::= {
  WITH SYNTAX             ACIItem
  EQUALITY MATCHING RULE  directoryStringFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-aca-entryACI
}

subentryACI ATTRIBUTE ::= {
  WITH SYNTAX             ACIItem
  EQUALITY MATCHING RULE  directoryStringFirstComponentMatch
  USAGE                   directoryOperation
  ID                      id-aca-subentryACI
}

-- object identifier assignments
-- attributes
id-aca-accessControlScheme OBJECT IDENTIFIER ::=
  {id-aca 1}

id-aca-prescriptiveACI OBJECT IDENTIFIER ::= {id-aca 4}

id-aca-entryACI OBJECT IDENTIFIER ::= {id-aca 5}

id-aca-subentryACI OBJECT IDENTIFIER ::= {id-aca 6}

-- access control schemes
basicAccessControlScheme OBJECT IDENTIFIER ::=
  {id-acScheme 1}

simplifiedAccessControlScheme OBJECT IDENTIFIER ::= {id-acScheme 2}

rule-based-access-control OBJECT IDENTIFIER ::= {id-acScheme 3}

rule-and-basic-access-control OBJECT IDENTIFIER ::= {id-acScheme 4}

rule-and-simple-access-control OBJECT IDENTIFIER ::= {id-acScheme 5}

END -- BasicAccessControl
```

Annex F

DSA Operational Attribute Types in ASN.1

Replace the ASN.1 module in Annex F with the following

```
DSAOperationalAttributeTypes {joint-iso-itu-t ds(5) module(1)
  dsaOperationalAttributeTypes(22) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
```

```
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  distributedOperations, id-doa, id-kmr, informationFramework,
    opBindingManagement, selectedAttributeTypes
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  ATTRIBUTE, MATCHING-RULE, Name
    FROM InformationFramework informationFramework
  OperationalBindingID
    FROM OperationalBindingManagement opBindingManagement
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  AccessPoint, DitBridgeKnowledge, MasterAndShadowAccessPoints
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  bitStringMatch, directoryStringFirstComponentMatch
    FROM SelectedAttributeTypes selectedAttributeTypes;

dseType ATTRIBUTE ::= {
  WITH SYNTAX             DSEType
  EQUALITY MATCHING RULE  bitStringMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-dseType
}

DSEType ::= BIT STRING {
  root(0), -- root DSE
  glue(1), -- represents knowledge of a name only
  cp(2), -- context prefix
  entry(3), -- object entry
  alias(4), -- alias entry
  subr(5), -- subordinate reference
  nssr(6), -- non-specific subordinate reference
  supr(7), -- superior reference
  xr(8), -- cross reference
  admPoint(9), -- administrative point
  subentry(10), -- subentry
  shadow(11), -- shadow copy
  immSupr(13), -- immediate superior reference
  rhob(14), -- rhob information
  sa(15), -- subordinate reference to alias entry
  dsSubentry(16), -- DSA Specific subentry
  familyMember(17), -- family member
  ditBridge(18), -- DIT bridge reference
  writeableCopy(19)} -- writeable copy

myAccessPoint ATTRIBUTE ::= {
  WITH SYNTAX             AccessPoint
  EQUALITY MATCHING RULE  accessPointMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-myAccessPoint
}

superiorKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             AccessPoint
  EQUALITY MATCHING RULE  accessPointMatch
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-superiorKnowledge
}

specificKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             MasterAndShadowAccessPoints
  EQUALITY MATCHING RULE  masterAndShadowAccessPointsMatch
  SINGLE VALUE            TRUE
  NO USER MODIFICATION    TRUE
```

```
  USAGE                   distributedOperation
  ID                      id-doa-specificKnowledge
}

nonSpecificKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             MasterAndShadowAccessPoints
  EQUALITY MATCHING RULE  masterAndShadowAccessPointsMatch
  NO USER MODIFICATION    TRUE
  USAGE                   distributedOperation
  ID                      id-doa-nonSpecificKnowledge
}

SupplierOrConsumer ::= SET {
  COMPONENTS OF AccessPoint, -- supplier or consumer
  agreementID  [3]  OperationalBindingID,
  ...
}

SupplierInformation ::= SET {
  COMPONENTS OF SupplierOrConsumer, -- supplier
  supplier-is-master    [4]  BOOLEAN DEFAULT TRUE,
  non-supplying-master  [5]  AccessPoint OPTIONAL,
  ...
}

supplierKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             SupplierInformation
  EQUALITY MATCHING RULE  supplierOrConsumerInformationMatch
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-supplierKnowledge
}

ConsumerInformation ::= SupplierOrConsumer -- consumer

consumerKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             ConsumerInformation
  EQUALITY MATCHING RULE  supplierOrConsumerInformationMatch
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-consumerKnowledge
}

SupplierAndConsumers ::= SET {
  COMPONENTS OF AccessPoint, -- supplier
  consumers  [3]  SET OF AccessPoint,
  ...
}

secondaryShadows ATTRIBUTE ::= {
  WITH SYNTAX             SupplierAndConsumers
  EQUALITY MATCHING RULE  supplierAndConsumersMatch
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-secondaryShadows
}

ditBridgeKnowledge ATTRIBUTE ::= {
  WITH SYNTAX             DitBridgeKnowledge
  EQUALITY MATCHING RULE  directoryStringFirstComponentMatch
  NO USER MODIFICATION    TRUE
  USAGE                   dSAOperation
  ID                      id-doa-ditBridgeKnowledge
}

-- matching rules
accessPointMatch MATCHING-RULE ::= {
  SYNTAX  Name
```

```
  ID      id-kmr-accessPointMatch
}

masterAndShadowAccessPointsMatch MATCHING-RULE ::= {
  SYNTAX  SET OF Name
  ID      id-kmr-masterShadowMatch
}

supplierOrConsumerInformationMatch MATCHING-RULE ::= {
  SYNTAX
    SET {ae-title              [0]  Name,
         agreement-identifier  [2]  INTEGER}
  ID      id-kmr-supplierConsumerMatch
}

supplierAndConsumersMatch MATCHING-RULE ::= {
  SYNTAX  Name
  ID      id-kmr-supplierConsumersMatch
}

-- object identifier assignments
-- dsa operational attributes
id-doa-dseType OBJECT IDENTIFIER ::=
  {id-doa 0}

id-doa-myAccessPoint OBJECT IDENTIFIER ::= {id-doa 1}

id-doa-superiorKnowledge OBJECT IDENTIFIER ::= {id-doa 2}

id-doa-specificKnowledge OBJECT IDENTIFIER ::= {id-doa 3}

id-doa-nonSpecificKnowledge OBJECT IDENTIFIER ::= {id-doa 4}

id-doa-supplierKnowledge OBJECT IDENTIFIER ::= {id-doa 5}

id-doa-consumerKnowledge OBJECT IDENTIFIER ::= {id-doa 6}

id-doa-secondaryShadows OBJECT IDENTIFIER ::= {id-doa 7}

id-doa-ditBridgeKnowledge OBJECT IDENTIFIER ::= {id-doa 8}

-- knowledge matching rules
id-kmr-accessPointMatch OBJECT IDENTIFIER ::=
  {id-kmr 0}

id-kmr-masterShadowMatch OBJECT IDENTIFIER ::= {id-kmr 1}

id-kmr-supplierConsumerMatch OBJECT IDENTIFIER ::= {id-kmr 2}

id-kmr-supplierConsumersMatch OBJECT IDENTIFIER ::= {id-kmr 3}

END -- DSAOperationalAttributeTypes
```

Annex G

Operational Binding Management in ASN.1

Replace the ASN.1 module in Annex G with the following

```
OperationalBindingManagement {joint-iso-itu-t ds(5) module(1)
  opBindingManagement(18) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
```

```
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryAbstractService, directoryShadowAbstractService,
    distributedOperations, directoryOSIProtocols, enhancedSecurity,
    hierarchicalOperationalBindings, commonProtocolSpecification
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  OPTIONALLY-PROTECTED-SEQ
    FROM EnhancedSecurity enhancedSecurity
  hierarchicalOperationalBinding, nonSpecificHierarchicalOperationalBinding
    FROM HierarchicalOperationalBindings hierarchicalOperationalBindings
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  CommonResultsSeq, directoryBind, securityError, SecurityParameters
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  AccessPoint
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  id-err-operationalBindingError, id-op-establishOperationalBinding,
    id-op-modifyOperationalBinding, id-op-terminateOperationalBinding,
    OPERATION, ERROR
    FROM CommonProtocolSpecification commonProtocolSpecification
  APPLICATION-CONTEXT
    FROM DirectoryOSIProtocols directoryOSIProtocols
  -- from ITU-T Rec. X.525 | ISO/IEC 9594-9
  shadowOperationalBinding
    FROM DirectoryShadowAbstractService directoryShadowAbstractService;

-- bind and unbind
dSAOperationalBindingManagementBind OPERATION ::=
  directoryBind

OPERATIONAL-BINDING ::= CLASS {
  &Agreement    ,
  &Cooperation  OP-BINDING-COOP,
  &both         OP-BIND-ROLE OPTIONAL,
  &roleA        OP-BIND-ROLE OPTIONAL,
  &roleB        OP-BIND-ROLE OPTIONAL,
  &id           OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  AGREEMENT &Agreement
  APPLICATION CONTEXTS &Cooperation
  [SYMMETRIC &both]
  [ASYMMETRIC
   [ROLE-A &roleA]
   [ROLE-B &roleB]]
  ID &id
}

OP-BINDING-COOP ::= CLASS {
  &applContext  APPLICATION-CONTEXT,
  &Operations   OPERATION OPTIONAL
}WITH SYNTAX {&applContext
              [APPLIES TO &Operations]
}

OP-BIND-ROLE ::= CLASS {
  &establish       BOOLEAN DEFAULT FALSE,
  &EstablishParam  OPTIONAL,
  &modify          BOOLEAN DEFAULT FALSE,
```

```
  &ModifyParam     OPTIONAL,
  &terminate       BOOLEAN DEFAULT FALSE,
  &TerminateParam  OPTIONAL
}
WITH SYNTAX {
  [ESTABLISHMENT-INITIATOR &establish]
  [ESTABLISHMENT-PARAMETER &EstablishParam]
  [MODIFICATION-INITIATOR &modify]
  [MODIFICATION-PARAMETER &ModifyParam]
  [TERMINATION-INITIATOR &terminate]
  [TERMINATION-PARAMETER &TerminateParam]
}

-- operations, arguments and results
establishOperationalBinding OPERATION ::= {
  ARGUMENT  EstablishOperationalBindingArgument
  RESULT    EstablishOperationalBindingResult
  ERRORS    {operationalBindingError | securityError}
  CODE      id-op-establishOperationalBinding
}

EstablishOperationalBindingArgument ::=
  OPTIONALLY-PROTECTED-SEQ
    {SEQUENCE {bindingType
                [0]  OPERATIONAL-BINDING.&id({OpBindingSet}),
               bindingID           [1]  OperationalBindingID OPTIONAL,
               accessPoint         [2]  AccessPoint,
               -- symmetric, Role A initiates, or Role B initiates
               initiator
                 CHOICE {symmetric
                           [3]  OPERATIONAL-BINDING.
                                  &both.&EstablishParam
                                  ({OpBindingSet}{@bindingType}),
                         roleA-initiates
                           [4]  OPERATIONAL-BINDING.
                                  &roleA.&EstablishParam
                                  ({OpBindingSet}{@bindingType}),
                         roleB-initiates
                           [5]  OPERATIONAL-BINDING.
                                  &roleB.&EstablishParam
                                  ({OpBindingSet}{@bindingType})} OPTIONAL,
               agreement
                 [6]  OPERATIONAL-BINDING.&Agreement
                        ({OpBindingSet}{@bindingType}),
               valid               [7]  Validity DEFAULT {},
               securityParameters  [8]  SecurityParameters OPTIONAL,
               ...}}

OpBindingSet OPERATIONAL-BINDING ::=
  {shadowOperationalBinding | hierarchicalOperationalBinding |
   nonSpecificHierarchicalOperationalBinding}

OperationalBindingID ::= SEQUENCE {identifier  INTEGER,
                                   version     INTEGER,
                                   ...
}

Validity ::= SEQUENCE {
  validFrom   [0]  CHOICE {now   [0]  NULL,
                           time  [1]  Time,
                           ...} DEFAULT now:NULL,
  validUntil
    [1]  CHOICE {explicitTermination  [0]  NULL,
                 time                 [1]  Time,
                 ...
  } DEFAULT explicitTermination:NULL,
  ...
}
```

```
Time ::= CHOICE {utcTime          UTCTime,
                 generalizedTime  GeneralizedTime,
                 ...
}

EstablishOperationalBindingResult ::=
  OPTIONALLY-PROTECTED-SEQ
    {SEQUENCE {bindingType  [0]  OPERATIONAL-BINDING.&id({OpBindingSet}),
               bindingID    [1]  OperationalBindingID OPTIONAL,
               accessPoint  [2]  AccessPoint,
               -- symmetric, Role A replies, or Role B replies
               initiator
                 CHOICE {symmetric
                           [3]  OPERATIONAL-BINDING.
                                  &both.&EstablishParam
                                  ({OpBindingSet}{@bindingType}),
                         roleA-replies
                           [4]  OPERATIONAL-BINDING.
                                  &roleA.&EstablishParam
                                  ({OpBindingSet}{@bindingType}),
                         roleB-replies
                           [5]  OPERATIONAL-BINDING.
                                  &roleB.&EstablishParam
                                  ({OpBindingSet}{@bindingType})} OPTIONAL,
               COMPONENTS OF CommonResultsSeq,
               ...}}

modifyOperationalBinding OPERATION ::= {
  ARGUMENT  ModifyOperationalBindingArgument
  RESULT    ModifyOperationalBindingResult
  ERRORS    {operationalBindingError | securityError}
  CODE      id-op-modifyOperationalBinding
}

ModifyOperationalBindingArgument ::=
  OPTIONALLY-PROTECTED-SEQ
    {SEQUENCE {bindingType
                 [0]  OPERATIONAL-BINDING.&id({OpBindingSet}),
               bindingID           [1]  OperationalBindingID,
               accessPoint         [2]  AccessPoint OPTIONAL,
               -- symmetric, Role A initiates, or Role B initiates
               initiator
                 CHOICE {symmetric
                           [3]  OPERATIONAL-BINDING.&both.&ModifyParam
                                  ({OpBindingSet}{@bindingType}),
                         roleA-initiates
                           [4]  OPERATIONAL-BINDING.&roleA.&ModifyParam
                                  ({OpBindingSet}{@bindingType}),
                         roleB-initiates
                           [5]  OPERATIONAL-BINDING.&roleB.&ModifyParam
                                  ({OpBindingSet}{@bindingType})} OPTIONAL,
               newBindingID        [6]  OperationalBindingID,
               newAgreement
                 [7]  OPERATIONAL-BINDING.&Agreement
                        ({OpBindingSet}{@bindingType}) OPTIONAL,
               valid               [8]  Validity OPTIONAL,
               securityParameters  [9]  SecurityParameters OPTIONAL,
               ...}}

ModifyOperationalBindingResult ::= CHOICE {
  null       [0]  NULL,
  protected
    [1]  OPTIONALLY-PROTECTED-SEQ{SEQUENCE {newBindingID  OperationalBindingID,
                                            bindingType
                                              OPERATIONAL-BINDING.&id
                                                ({OpBindingSet}),
                                            newAgreement
```

```
                                        OPERATIONAL-BINDING.
                                          &Agreement
                                          ({OpBindingSet}{@.bindingType}),
                                      valid         Validity OPTIONAL,
                                      COMPONENTS OF CommonResultsSeq,
                                      ...
          }},
  ...
}

terminateOperationalBinding OPERATION ::= {
  ARGUMENT  TerminateOperationalBindingArgument
  RESULT    TerminateOperationalBindingResult
  ERRORS    {operationalBindingError | securityError}
  CODE      id-op-terminateOperationalBinding
}

TerminateOperationalBindingArgument ::=
  OPTIONALLY-PROTECTED-SEQ
    {SEQUENCE {bindingType
                [0]  OPERATIONAL-BINDING.&id({OpBindingSet}),
              bindingID           [1]  OperationalBindingID,
              -- symmetric, Role A initiates, or Role B initiates
              initiator
                CHOICE {symmetric
                          [2]  OPERATIONAL-BINDING.
                                 &both.&TerminateParam
                                 ({OpBindingSet}{@bindingType}),
                        roleA-initiates
                          [3]  OPERATIONAL-BINDING.
                                 &roleA.&TerminateParam
                                 ({OpBindingSet}{@bindingType}),
                        roleB-initiates
                          [4]  OPERATIONAL-BINDING.
                                 &roleB.&TerminateParam
                                 ({OpBindingSet}{@bindingType})} OPTIONAL,
              terminateAt         [5]  Time OPTIONAL,
              securityParameters  [6]  SecurityParameters OPTIONAL,
              ...}}

TerminateOperationalBindingResult ::= CHOICE {
  null       [0]  NULL,
  protected
    [1]  OPTIONALLY-PROTECTED-SEQ{SEQUENCE {bindingID    OperationalBindingID,
                                      bindingType
                                        OPERATIONAL-BINDING.&id
                                          ({OpBindingSet}),
                                      terminateAt
                                        GeneralizedTime OPTIONAL,
                                      COMPONENTS OF CommonResultsSeq,
                                      ...
          }},
  ...
}

-- errors and parameters
operationalBindingError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED-SEQ  {OpBindingErrorParam}
  CODE                                id-err-operationalBindingError
}

OpBindingErrorParam ::= SEQUENCE {
  problem
    [0]  ENUMERATED {invalidID(0), duplicateID(1), unsupportedBindingType(2),
                     notAllowedForRole(3), parametersMissing(4),
                     roleAssignment(5), invalidStartTime(6), invalidEndTime(7),
                     invalidAgreement(8), currentlyNotDecidable(9),
                     modificationNotAllowed(10),...},
```

```
  bindingType        [1]  OPERATIONAL-BINDING.&id({OpBindingSet}) OPTIONAL,
  agreementProposal
    [2]  OPERATIONAL-BINDING.&Agreement({OpBindingSet}{@bindingType})
      OPTIONAL,
  retryAt            [3]  Time OPTIONAL,
  COMPONENTS OF CommonResultsSeq,
  ...
}

END -- OperationalBindingManagement
```

Annex H

Enhanced security

Replace the ASN.1 module in Annex H with the following

```
EnhancedSecurity {joint-iso-itu-t ds(5) modules(1) enhancedSecurity(28) 6}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS All
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  authenticationFramework, basicAccessControl, certificateExtensions,
    id-at, id-avc, id-mr, id-oc, informationFramework
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Attribute{}, ATTRIBUTE, AttributeType, Context, CONTEXT, MATCHING-RULE,
    Name, OBJECT-CLASS, objectIdentifierMatch, SupportedAttributes, top
    FROM InformationFramework informationFramework
  AttributeTypeAndValue
    FROM BasicAccessControl basicAccessControl
  -- from ITU-T Rec. X.509 | ISO/IEC 9594-8
  CertificateSerialNumber, HASH{}, SIGNED{}
    FROM AuthenticationFramework authenticationFramework
  GeneralName, KeyIdentifier
    FROM CertificateExtensions certificateExtensions;

--   ub-privacy-mark-length
--        FROM UpperBounds upperBounds;
OPTIONALLY-PROTECTED{Type} ::= CHOICE {unsigned  Type,
                                       signed    SIGNED{Type}
}

OPTIONALLY-PROTECTED-SEQ{Type} ::= CHOICE {
  unsigned  Type,
  signed    [0]  SIGNED{Type}
}

attributeValueSecurityLabelContext CONTEXT ::= {
  WITH SYNTAX
    SignedSecurityLabel --  At most one security label context can be assigned to an
  --  attribute value
  ID           id-avc-attributeValueSecurityLabelContext
}

SignedSecurityLabel ::= SIGNED{SignedSecurityLabelContent}

SignedSecurityLabelContent ::= SEQUENCE {
  attHash        HASH{AttributeTypeAndValue},
  issuer         Name OPTIONAL, -- name of labelling authority
  keyIdentifier  KeyIdentifier OPTIONAL,
  securityLabel  SecurityLabel,
```

```
  ...
}

SecurityLabel ::= SET {
  security-policy-identifier  SecurityPolicyIdentifier OPTIONAL,
  security-classification     SecurityClassification OPTIONAL,
  privacy-mark                PrivacyMark OPTIONAL,
  security-categories         SecurityCategories OPTIONAL,
  ...
}(ALL EXCEPT ({ -- none, at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
  unmarked(0), unclassified(1), restricted(2), confidential(3), secret(4),
  top-secret(5)}

PrivacyMark ::= PrintableString(SIZE (1..MAX))

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

clearance ATTRIBUTE ::= {WITH SYNTAX  Clearance
                         ID           id-at-clearance
}

Clearance ::= SEQUENCE {
  policyId            OBJECT IDENTIFIER,
  classList           ClassList DEFAULT {unclassified},
  securityCategories  SET SIZE (1..MAX) OF SecurityCategory OPTIONAL,
  ...
}

ClassList ::= BIT STRING {
  unmarked(0), unclassified(1), restricted(2), confidential(3), secret(4),
  topSecret(5)}

SecurityCategory ::= SEQUENCE {
  type   [0]  SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
  value
    [1] EXPLICIT SECURITY-CATEGORY.&Type({SecurityCategoriesTable}{@type}),
  ...
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::=
  {...}

attributeIntegrityInfo ATTRIBUTE ::= {
  WITH SYNTAX   AttributeIntegrityInfo
  SINGLE VALUE  TRUE
  ID            id-at-attributeIntegrityInfo
}

AttributeIntegrityInfo ::= SIGNED{AttributeIntegrityInfoContent}

AttributeIntegrityInfoContent ::= SEQUENCE {
  scope        Scope, -- Identifies the attributes protected
  signer       Signer OPTIONAL, -- Authority or data originators name
  attribsHash  AttribsHash,
  ...
} -- Hash value of protected attributes

Signer ::= CHOICE {
  thisEntry   [0] EXPLICIT ThisEntry,
  thirdParty  [1]  SpecificallyIdentified,
  ...
}
```

```
ThisEntry ::= CHOICE {onlyOne   NULL,
                      specific  IssuerAndSerialNumber,
                      ...
}

IssuerAndSerialNumber ::= SEQUENCE {
  issuer  Name,
  serial  CertificateSerialNumber,
  ...
}

SpecificallyIdentified ::= SEQUENCE {
  name    GeneralName,
  issuer  GeneralName OPTIONAL,
  serial  CertificateSerialNumber OPTIONAL
}
(WITH COMPONENTS {
   ...,
   issuer  PRESENT,
   serial  PRESENT
 } | (WITH COMPONENTS {
        ...,
        issuer  ABSENT,
        serial  ABSENT
      }))

Scope ::= CHOICE {
  wholeEntry     [0]  NULL, -- Signature protects all attribute values in this entry
  selectedTypes  [1]  SelectedTypes,
  -- Signature protects all attribute values of the selected attribute types
  ...
}

SelectedTypes ::= SEQUENCE SIZE (1..MAX) OF AttributeType

AttribsHash ::= HASH{HashedAttributes}

HashedAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}}

-- Attribute type and values with associated context values for the selected Scope
integrityInfo OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          auxiliary
  MUST CONTAIN  {attributeIntegrityInfo}
  ID            id-oc-integrityInfo
}

attributeValueIntegrityInfoContext CONTEXT ::= {
  WITH SYNTAX  AttributeValueIntegrityInfo
  ID           id-avc-attributeValueIntegrityInfoContext
}

AttributeValueIntegrityInfo ::= SIGNED{AttributeValueIntegrityInfoContent}

AttributeValueIntegrityInfoContent ::= SEQUENCE {
  signer   Signer OPTIONAL, -- Authority or data originators name
  aVIHash  AVIHash,
  ...
} -- Hash value of protected attribute

AVIHash ::= HASH{AttributeTypeValueContexts}

-- Attribute type and value with associated context values
AttributeTypeValueContexts ::= SEQUENCE {
  type         ATTRIBUTE.&id({SupportedAttributes}),
  value        ATTRIBUTE.&Type({SupportedAttributes}{@type}),
  contextList  SET SIZE (1..MAX) OF Context OPTIONAL,
```

```
  ...
}

-- Object identifier assignments
-- object classes
id-oc-integrityInfo OBJECT IDENTIFIER ::=
  {id-oc 40}

-- attributes
id-at-clearance OBJECT IDENTIFIER ::= {id-at 55}

-- id-at-defaultDirQop                    OBJECT IDENTIFIER  ::=  {id-at 56}
id-at-attributeIntegrityInfo OBJECT IDENTIFIER ::=
  {id-at 57}

-- id-at-confKeyInfo                           OBJECT IDENTIFIER  ::=  {id-at 60}
-- matching rules
-- id-mr-readerAndKeyIDMatch              OBJECT IDENTIFIER  ::=  {id-mr 43}
-- contexts
id-avc-attributeValueSecurityLabelContext OBJECT IDENTIFIER ::=
  {id-avc 3}

id-avc-attributeValueIntegrityInfoContext OBJECT IDENTIFIER ::= {id-avc 4}

END -- EnhancedSecurity
```

ISO/IEC 9594-3 : 2008, Information Technology - Open systems Interconnection - The Directory: Abstract Service Definition

Working draft for Amendment 1: Communications support enhancements

Annex A

Abstract Service in ASN.1

Replace the ASN.1 module in Annex A with the following

```
DirectoryAbstractService {joint-iso-itu-t ds(5) module(1)
  directoryAbstractService(2) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  attributeCertificateDefinitions, authenticationFramework, basicAccessControl,
    commonProtocolSpecification, directoryShadowAbstractService,
    distributedOperations, enhancedSecurity, id-at, informationFramework,
    selectedAttributeTypes, serviceAdministration
```

```
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Attribute{}, ATTRIBUTE, AttributeType, AttributeTypeAssertion,
    AttributeValue, AttributeValueAssertion, CONTEXT, ContextAssertion,
    DistinguishedName, MATCHING-RULE, Name, OBJECT-CLASS,
    RelativeDistinguishedName, SupportedAttributes, SupportedContexts
    FROM InformationFramework informationFramework
  RelaxationPolicy
    FROM ServiceAdministration serviceAdministration
  AttributeTypeAndValue
    FROM BasicAccessControl basicAccessControl
  OPTIONALLY-PROTECTED{}, OPTIONALLY-PROTECTED-SEQ{}
    FROM EnhancedSecurity enhancedSecurity
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  AccessPoint, ContinuationReference, Exclusions, OperationProgress,
    ReferenceType
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  Code, ERROR, id-errcode-abandoned, id-errcode-abandonFailed,
    id-errcode-attributeError, id-errcode-nameError, id-errcode-referral,
    id-errcode-securityError, id-errcode-serviceError, id-errcode-updateError,
    id-opcode-abandon, id-opcode-addEntry, id-opcode-compare, id-opcode-list,
    id-opcode-modifyDN, id-opcode-modifyEntry, id-opcode-read,
    id-opcode-removeEntry, id-opcode-search, InvokeId, OPERATION
    FROM CommonProtocolSpecification commonProtocolSpecification
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  DirectoryString{}, UnboundedDirectoryString
    FROM SelectedAttributeTypes selectedAttributeTypes
  -- from ITU-T Rec. X.509 | ISO/IEC 9594-8
  AlgorithmIdentifier{}, CertificationPath, ENCRYPTED{}, HASH{}, SIGNED{},
    SupportedAlgorithms
    FROM AuthenticationFramework authenticationFramework
  AttributeCertificationPath
    FROM AttributeCertificateDefinitions attributeCertificateDefinitions
  -- from ITU-T Rec. X.525 | ISO/IEC 9594-9
  AgreementID
    FROM DirectoryShadowAbstractService directoryShadowAbstractService
  -- from RFC 2025
  SPKM-ERROR, SPKM-REP-TI, SPKM-REQ
    FROM SpkmGssTokens {iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) spkm(1) spkmGssTokens(10)};

-- Common data types
CommonArguments ::= SET {
  serviceControls      [30]  ServiceControls DEFAULT {},
  securityParameters   [29]  SecurityParameters OPTIONAL,
  requestor            [28]  DistinguishedName OPTIONAL,
  operationProgress
    [27]  OperationProgress DEFAULT {nameResolutionPhase notStarted},
  aliasedRDNs          [26]  INTEGER OPTIONAL,
  criticalExtensions   [25]  BIT STRING OPTIONAL,
  referenceType        [24]  ReferenceType OPTIONAL,
  entryOnly            [23]  BOOLEAN DEFAULT TRUE,
  exclusions           [22]  Exclusions OPTIONAL,
  nameResolveOnMaster  [21]  BOOLEAN DEFAULT FALSE,
  operationContexts    [20]  ContextSelection OPTIONAL,
  familyGrouping       [19]  FamilyGrouping DEFAULT entryOnly,
  ...
}

FamilyGrouping ::= ENUMERATED {
  entryOnly(1), compoundEntry(2), strands(3), multiStrand(4),...}

CommonResults ::= SET {
  securityParameters  [30]  SecurityParameters OPTIONAL,
  performer           [29]  DistinguishedName OPTIONAL,
  aliasDereferenced   [28]  BOOLEAN DEFAULT FALSE,
  notification
```

```
    [27]  SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  ...
}

CommonResultsSeq ::= SEQUENCE {
  securityParameters  [30]  SecurityParameters OPTIONAL,
  performer           [29]  DistinguishedName OPTIONAL,
  aliasDereferenced   [28]  BOOLEAN DEFAULT FALSE,
  notification
    [27]  SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  ...
}

ServiceControls ::= SET {
  options              [0]  ServiceControlOptions DEFAULT {},
  priority             [1]  INTEGER {low(0), medium(1), high(2)} DEFAULT medium,
  timeLimit            [2]  INTEGER OPTIONAL,
  sizeLimit            [3]  INTEGER OPTIONAL,
  scopeOfReferral      [4]  INTEGER {dmd(0), country(1)} OPTIONAL,
  attributeSizeLimit   [5]  INTEGER OPTIONAL,
  manageDSAITPlaneRef
    [6]  SEQUENCE {dsaName      Name,
                   agreementID  AgreementID,
                   ...} OPTIONAL,
  serviceType          [7]  OBJECT IDENTIFIER OPTIONAL,
  userClass            [8]  INTEGER OPTIONAL,
  ...
}

ServiceControlOptions ::= BIT STRING {
  preferChaining(0), chainingProhibited(1), localScope(2), dontUseCopy(3),
  dontDereferenceAliases(4), subentries(5), copyShallDo(6),
  partialNameResolution(7), manageDSAIT(8), noSubtypeMatch(9),
  noSubtypeSelection(10), countFamily(11), dontSelectFriends(12),
  dontMatchFriends(13)}

EntryInformationSelection ::= SET {
  attributes
    CHOICE {allUserAttributes  [0]  NULL,
            select             [1]  SET OF AttributeType
            --  empty set implies no attributes are requested
  } DEFAULT allUserAttributes:NULL,
  infoTypes
    [2]  INTEGER {attributeTypesOnly(0), attributeTypesAndValues(1)}
      DEFAULT attributeTypesAndValues,
  extraAttributes
    CHOICE {allOperationalAttributes  [3]  NULL,
            select                    [4]  SET SIZE (1..MAX) OF AttributeType
  } OPTIONAL,
  contextSelection  ContextSelection OPTIONAL,
  returnContexts    BOOLEAN DEFAULT FALSE,
  familyReturn      FamilyReturn DEFAULT {memberSelect contributingEntriesOnly}
}

ContextSelection ::= CHOICE {
  allContexts       NULL,
  selectedContexts  SET SIZE (1..MAX) OF TypeAndContextAssertion,
  ...
}

TypeAndContextAssertion ::= SEQUENCE {
  type               AttributeType,
  contextAssertions
    CHOICE {preference  SEQUENCE OF ContextAssertion,
            all         SET OF ContextAssertion,
            ...},
  ...
}
```

```
FamilyReturn ::= SEQUENCE {
  memberSelect
    ENUMERATED {contributingEntriesOnly(1), participatingEntriesOnly(2),
                compoundEntry(3),...},
  familySelect  SEQUENCE SIZE (1..MAX) OF OBJECT-CLASS.&id OPTIONAL,
  ...
}

EntryInformation ::= SEQUENCE {
  name             Name,
  fromEntry        BOOLEAN DEFAULT TRUE,
  information
    SET SIZE (1..MAX) OF
      CHOICE {attributeType  AttributeType,
              attribute      Attribute{{SupportedAttributes}},
              ...} OPTIONAL,
  incompleteEntry  [3]  BOOLEAN DEFAULT FALSE, -- not in first edition systems
  partialName      [4]  BOOLEAN DEFAULT FALSE, -- not in first or second edition systems
  derivedEntry
    [5]  BOOLEAN DEFAULT FALSE, -- not in pre-fourth edition systems --
...
}

family-information ATTRIBUTE ::= {
  WITH SYNTAX  FamilyEntries
  USAGE        directoryOperation
  ID           id-at-family-information
}

FamilyEntries ::= SEQUENCE {
  family-class   OBJECT-CLASS.&id, -- structural object class value
  familyEntries  SEQUENCE OF FamilyEntry,
  ...
}

FamilyEntry ::= SEQUENCE {
  rdn          RelativeDistinguishedName,
  information
    SEQUENCE OF
      CHOICE {attributeType  AttributeType,
              attribute      Attribute{{SupportedAttributes}},
              ...},
  family-info  SEQUENCE SIZE (1..MAX) OF FamilyEntries OPTIONAL,
  ...
}

Filter ::= CHOICE {
  item  [0]  FilterItem,
  and   [1]  SET OF Filter,
  or    [2]  SET OF Filter,
  not   [3]  Filter,
  ...
}

FilterItem ::= CHOICE {
  equality          [0]  AttributeValueAssertion,
  substrings
    [1]  SEQUENCE {type     ATTRIBUTE.&id({SupportedAttributes}),
                   strings
                     SEQUENCE OF
                       CHOICE {initial
                                 [0]  ATTRIBUTE.&Type
                                        ({SupportedAttributes}
                                           {@substrings.type}),
                               any
                                 [1]  ATTRIBUTE.&Type
                                        ({SupportedAttributes}
```

```
                                        {@substrings.type}),
                                final
                                  [2]  ATTRIBUTE.&Type
                                         ({SupportedAttributes}
                                           {@substrings.type}),
                                control  Attribute{{SupportedAttributes}},
                                ...
                           },
                        ...
                        }, -- Used to specify interpretation of following

  -- items
  greaterOrEqual    [2]  AttributeValueAssertion,
  lessOrEqual       [3]  AttributeValueAssertion,
  present           [4]  AttributeType,
  approximateMatch  [5]  AttributeValueAssertion,
  extensibleMatch   [6]  MatchingRuleAssertion,
  contextPresent    [7]  AttributeTypeAssertion,
  ...
}

MatchingRuleAssertion ::= SEQUENCE {
  matchingRule  [1]  SET SIZE (1..MAX) OF MATCHING-RULE.&id,
  type          [2]  AttributeType OPTIONAL,
  matchValue
    [3]  MATCHING-RULE.&AssertionType
           (CONSTRAINED BY {
              -- matchValue shall be a value of  type specified by the &AssertionType
field of
              -- one of the MATCHING-RULE information objects identified by matchingRule
-- }),
  dnAttributes  [4]  BOOLEAN DEFAULT FALSE,
  ...
}

PagedResultsRequest ::= CHOICE {
  newRequest
    SEQUENCE {pageSize    INTEGER,
              sortKeys    SEQUENCE SIZE (1..MAX) OF SortKey OPTIONAL,
              reverse     [1]  BOOLEAN DEFAULT FALSE,
              unmerged    [2]  BOOLEAN DEFAULT FALSE,
              pageNumber  [3]  INTEGER OPTIONAL,
              ...},
  queryReference  OCTET STRING,
  abandonQuery    [0]  OCTET STRING,
  ...
}

SortKey ::= SEQUENCE {
  type          AttributeType,
  orderingRule  MATCHING-RULE.&id OPTIONAL,
  ...
}

SecurityParameters ::= SET {
  certification-path          [0]  CertificationPath OPTIONAL,
  name                        [1]  DistinguishedName OPTIONAL,
  time                        [2]  Time OPTIONAL,
  random                      [3]  BIT STRING OPTIONAL,
  target                      [4]  ProtectionRequest OPTIONAL,
  response                    [5]  BIT STRING OPTIONAL,
  operationCode               [6]  Code OPTIONAL,
  attributeCertificationPath  [7]  AttributeCertificationPath OPTIONAL,
  errorProtection             [8]  ErrorProtectionRequest OPTIONAL,
  errorCode                   [9]  Code OPTIONAL,
  ...
}
```

```
ProtectionRequest ::= INTEGER {none(0), signed(1)}

Time ::= CHOICE {utcTime          UTCTime,
                 generalizedTime  GeneralizedTime,
                 ...
}

ErrorProtectionRequest ::= INTEGER {none(0), signed(1)}

--  Bind and unbind operations
directoryBind OPERATION ::= {
  ARGUMENT  DirectoryBindArgument
  RESULT    DirectoryBindResult
  ERRORS    {directoryBindError}
}

DirectoryBindArgument ::= SET {
  credentials  [0]  Credentials OPTIONAL,
  versions     [1]  Versions DEFAULT {v1},
  ...
}

Credentials ::= CHOICE {
  simple             [0]  SimpleCredentials,
  strong             [1]  StrongCredentials,
  externalProcedure  [2]  EXTERNAL,
  spkm               [3]  SpkmCredentials,
  sasl               [4]  SaslCredentials,
  ...
}

SimpleCredentials ::= SEQUENCE {
  name      [0]  DistinguishedName,
  validity
    [1]  SET {time1    [0]  CHOICE {utc  UTCTime,
                                    gt   GeneralizedTime} OPTIONAL,
              time2    [1]  CHOICE {utc  UTCTime,
                                    gt   GeneralizedTime} OPTIONAL,
              random1  [2]  BIT STRING OPTIONAL,
              random2  [3]  BIT STRING OPTIONAL} OPTIONAL,
  password
    [2]  CHOICE {unprotected  OCTET STRING,
                 protected    HASH{OCTET STRING}} OPTIONAL,
  ...
}

StrongCredentials ::= SET {
  certification-path          [0]  CertificationPath OPTIONAL,
  bind-token                  [1]  Token,
  name                        [2]  DistinguishedName OPTIONAL,
  attributeCertificationPath  [3]  AttributeCertificationPath OPTIONAL,
  ...
}

SpkmCredentials ::= CHOICE {req  [0]  SPKM-REQ,
                            rep  [1]  SPKM-REP-TI,
                            ...
}

SaslCredentials ::= SEQUENCE {
  mechanism    [0]  DirectoryString{ub-saslMechanism},
  credentials  [1]  OCTET STRING OPTIONAL,
  saslAbort    [2]  BOOLEAN DEFAULT FALSE,
  ...
}

ub-saslMechanism INTEGER ::= 20 -- According to RFC 2222
```

```
Token ::= SIGNED{TokenContent}

TokenContent ::= SEQUENCE {
  algorithm  [0]  AlgorithmIdentifier{{SupportedAlgorithms}},
  name       [1]  DistinguishedName,
  time       [2]  Time,
  random     [3]  BIT STRING,
  response   [4]  BIT STRING OPTIONAL,
  ...
}

Versions ::= BIT STRING {v1(0), v2(1)}

DirectoryBindResult ::= DirectoryBindArgument

directoryBindError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {versions            [0]  Versions DEFAULT {v1},
          error
            CHOICE {serviceError   [1]  ServiceProblem,
                    securityError  [2]  SecurityProblem,
                    ...},
          securityParameters  [30]  SecurityParameters OPTIONAL
          }}
}

BindKeyInfo ::= ENCRYPTED{BIT STRING}

--  Operations, arguments, and results
read OPERATION ::= {
  ARGUMENT  ReadArgument
  RESULT    ReadResult
  ERRORS
    {attributeError | nameError | serviceError | referral | abandoned |
      securityError}
  CODE      id-opcode-read
}

ReadArgument ::=
  OPTIONALLY-PROTECTED
    {SET {object               [0]  Name,
          selection            [1]  EntryInformationSelection DEFAULT {},
          modifyRightsRequest  [2]  BOOLEAN DEFAULT FALSE,
          COMPONENTS OF CommonArguments,
          ...}}

ReadResult ::=
  OPTIONALLY-PROTECTED
    {SET {entry         [0]  EntryInformation,
          modifyRights  [1]  ModifyRights OPTIONAL,
          COMPONENTS OF CommonResults,
          ...}}

ModifyRights ::=
  SET OF
    SEQUENCE {item
                CHOICE {entry      [0]  NULL,
                        attribute  [1]  AttributeType,
                        value      [2]  AttributeValueAssertion,
                        ...},
              permission
                [3]  BIT STRING {add(0), remove(1), rename(2), move(3)},
              ...
    }

compare OPERATION ::= {
  ARGUMENT  CompareArgument
  RESULT    CompareResult
```

```
  ERRORS
    {attributeError | nameError | serviceError | referral | abandoned |
      securityError}
  CODE      id-opcode-compare
}

CompareArgument ::=
  OPTIONALLY-PROTECTED
    {SET {object     [0]  Name,
          purported  [1]  AttributeValueAssertion,
          COMPONENTS OF CommonArguments,
          ...}}

CompareResult ::=
  OPTIONALLY-PROTECTED
    {SET {name            Name OPTIONAL,
          matched         [0]  BOOLEAN,
          fromEntry       [1]  BOOLEAN DEFAULT TRUE,
          matchedSubtype  [2]  AttributeType OPTIONAL,
          COMPONENTS OF CommonResults,
          ...}}

abandon OPERATION ::= {
  ARGUMENT  AbandonArgument
  RESULT    AbandonResult
  ERRORS    {abandonFailed}
  CODE      id-opcode-abandon
}

AbandonArgument ::=
  OPTIONALLY-PROTECTED-SEQ{SEQUENCE {invokeID  [0]  InvokeId,
                                     ...}}

AbandonResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED-SEQ{SEQUENCE {invokeID  InvokeId,
                                       COMPONENTS OF CommonResultsSeq,
                                       ...
      }},
  ...
}

list OPERATION ::= {
  ARGUMENT  ListArgument
  RESULT    ListResult
  ERRORS    {nameError | serviceError | referral | abandoned | securityError}
  CODE      id-opcode-list
}

ListArgument ::=
  OPTIONALLY-PROTECTED
    {SET {object        [0]  Name,
          pagedResults  [1]  PagedResultsRequest OPTIONAL,
          listFamily    [2]  BOOLEAN DEFAULT FALSE,
          COMPONENTS OF CommonArguments,
          ...}}

ListResult ::=
  OPTIONALLY-PROTECTED
    {CHOICE {listInfo
               SET {name                     Name OPTIONAL,
                    subordinates
                      [1]  SET OF
                             SEQUENCE {rdn         RelativeDistinguishedName,
                                       aliasEntry  [0]  BOOLEAN DEFAULT FALSE,
                                       fromEntry   [1]  BOOLEAN DEFAULT TRUE,
                                       ...
```

```
                    },
                partialOutcomeQualifier
                  [2]  PartialOutcomeQualifier OPTIONAL,
                COMPONENTS OF CommonResults,
                ...},
            uncorrelatedListInfo  [0]  SET OF ListResult,
            ...}}

PartialOutcomeQualifier ::= SET {
  limitProblem                  [0]  LimitProblem OPTIONAL,
  unexplored
    [1]  SET SIZE (1..MAX) OF ContinuationReference OPTIONAL,
  unavailableCriticalExtensions  [2]  BOOLEAN DEFAULT FALSE,
  unknownErrors
    [3]  SET SIZE (1..MAX) OF ABSTRACT-SYNTAX.&Type OPTIONAL,
  queryReference                [4]  OCTET STRING OPTIONAL,
  overspecFilter                [5]  Filter OPTIONAL,
  notification
    [6]  SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  entryCount
    CHOICE {bestEstimate  [7]  INTEGER,
            lowEstimate   [8]  INTEGER,
            exact         [9]  INTEGER,
            ...} OPTIONAL,
  streamedResult                [10]  BOOLEAN DEFAULT FALSE
}

LimitProblem ::= INTEGER {
  timeLimitExceeded(0), sizeLimitExceeded(1), administrativeLimitExceeded(2)
}

search OPERATION ::= {
  ARGUMENT  SearchArgument
  RESULT    SearchResult
  ERRORS
    {attributeError | nameError | serviceError | referral | abandoned |
      securityError}
  CODE      id-opcode-search
}

SearchArgument ::=
  OPTIONALLY-PROTECTED
    {SET {baseObject           [0]  Name,
          subset
            [1]  INTEGER {baseObject(0), oneLevel(1), wholeSubtree(2)}
              DEFAULT baseObject,
          filter               [2]  Filter DEFAULT and:{},
          searchAliases        [3]  BOOLEAN DEFAULT TRUE,
          selection            [4]  EntryInformationSelection DEFAULT {},
          pagedResults         [5]  PagedResultsRequest OPTIONAL,
          matchedValuesOnly    [6]  BOOLEAN DEFAULT FALSE,
          extendedFilter       [7]  Filter OPTIONAL,
          checkOverspecified   [8]  BOOLEAN DEFAULT FALSE,
          relaxation           [9]  RelaxationPolicy OPTIONAL,
          extendedArea         [10]  INTEGER OPTIONAL,
          hierarchySelections  [11]  HierarchySelections DEFAULT {self},
          searchControlOptions
            [12]  SearchControlOptions DEFAULT {searchAliases},
          joinArguments
            [13]  SEQUENCE SIZE (1..MAX) OF JoinArgument OPTIONAL,
          joinType
            [14]  ENUMERATED {innerJoin(0), leftOuterJoin(1), fullOuterJoin(2)}
              DEFAULT leftOuterJoin,
          COMPONENTS OF CommonArguments,
          ...}}

HierarchySelections ::= BIT STRING {
  self(0), children(1), parent(2), hierarchy(3), top(4), subtree(5),
```

```
  siblings(6), siblingChildren(7), siblingSubtree(8), all(9)}

SearchControlOptions ::= BIT STRING {
  searchAliases(0), matchedValuesOnly(1), checkOverspecified(2),
  performExactly(3), includeAllAreas(4), noSystemRelaxation(5), dnAttribute(6),
  matchOnResidualName(7), entryCount(8), useSubset(9),
  separateFamilyMembers(10), searchFamily(11)}

JoinArgument ::= SEQUENCE {
  joinBaseObject  [0]  Name,
  domainLocalID   [1]  DomainLocalID OPTIONAL,
  joinSubset
    [2]  ENUMERATED {baseObject(0), oneLevel(1), wholeSubtree(2),...}
      DEFAULT baseObject,
  joinFilter      [3]  Filter OPTIONAL,
  joinAttributes  [4]  SEQUENCE SIZE (1..MAX) OF JoinAttPair OPTIONAL,
  joinSelection   [5]  EntryInformationSelection,
  ...
}

DomainLocalID ::= UnboundedDirectoryString

JoinAttPair ::= SEQUENCE {
  baseAtt      AttributeType,
  joinAtt      AttributeType,
  joinContext  SEQUENCE SIZE (1..MAX) OF JoinContextType OPTIONAL,
  ...
}

JoinContextType ::= CONTEXT.&id({SupportedContexts})

SearchResult ::=
  OPTIONALLY-PROTECTED
    {CHOICE {searchInfo
               SET {name                      Name OPTIONAL,
                    entries                   [0]  SET OF EntryInformation,
                    partialOutcomeQualifier
                      [2]  PartialOutcomeQualifier OPTIONAL,
                    altMatching               [3]  BOOLEAN DEFAULT FALSE,
                    COMPONENTS OF CommonResults,
                    ...},
             uncorrelatedSearchInfo  [0]  SET OF SearchResult,
             ...}}

addEntry OPERATION ::= {
  ARGUMENT  AddEntryArgument
  RESULT    AddEntryResult
  ERRORS
    {attributeError | nameError | serviceError | referral | securityError |
      updateError}
  CODE      id-opcode-addEntry
}

AddEntryArgument ::=
  OPTIONALLY-PROTECTED
    {SET {object        [0]  Name,
          entry         [1]  SET OF Attribute{{SupportedAttributes}},
          targetSystem  [2]  AccessPoint OPTIONAL,
          COMPONENTS OF CommonArguments,
          ...}}

AddEntryResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED-SEQ{SEQUENCE {COMPONENTS OF CommonResultsSeq,
                                       ...}},
  ...
}
```

```
removeEntry OPERATION ::= {
  ARGUMENT  RemoveEntryArgument
  RESULT    RemoveEntryResult
  ERRORS    {nameError | serviceError | referral | securityError | updateError}
  CODE      id-opcode-removeEntry
}

RemoveEntryArgument ::=
  OPTIONALLY-PROTECTED{SET {object  [0]  Name,
                            COMPONENTS OF CommonArguments,
                            ...}}

RemoveEntryResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED-SEQ{SEQUENCE {COMPONENTS OF CommonResultsSeq,
                                       ...}},
  ...
}

modifyEntry OPERATION ::= {
  ARGUMENT  ModifyEntryArgument
  RESULT    ModifyEntryResult
  ERRORS
    {attributeError | nameError | serviceError | referral | securityError |
      updateError}
  CODE      id-opcode-modifyEntry
}

ModifyEntryArgument ::=
  OPTIONALLY-PROTECTED
    {SET {object     [0]  Name,
          changes    [1]  SEQUENCE OF EntryModification,
          selection  [2]  EntryInformationSelection OPTIONAL,
          COMPONENTS OF CommonArguments,
          ...}}

ModifyEntryResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED-SEQ{SEQUENCE {entry  [0]  EntryInformation OPTIONAL,
                                       COMPONENTS OF CommonResultsSeq,
                                       ...
      }},
  ...
}

EntryModification ::= CHOICE {
  addAttribute     [0]  Attribute{{SupportedAttributes}},
  removeAttribute  [1]  AttributeType,
  addValues        [2]  Attribute{{SupportedAttributes}},
  removeValues     [3]  Attribute{{SupportedAttributes}},
  alterValues      [4]  AttributeTypeAndValue,
  resetValue       [5]  AttributeType,
  replaceValues    [6]  Attribute{{SupportedAttributes}},
  ...
}

modifyDN OPERATION ::= {
  ARGUMENT  ModifyDNArgument
  RESULT    ModifyDNResult
  ERRORS    {nameError | serviceError | referral | securityError | updateError}
  CODE      id-opcode-modifyDN
}

ModifyDNArgument ::=
  OPTIONALLY-PROTECTED
```

```
    {SET {object        [0]  DistinguishedName,
          newRDN        [1]  RelativeDistinguishedName,
          deleteOldRDN  [2]  BOOLEAN DEFAULT FALSE,
          newSuperior   [3]  DistinguishedName OPTIONAL,
          COMPONENTS OF CommonArguments,
          ...}}

ModifyDNResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED-SEQ{SEQUENCE {newRDN  RelativeDistinguishedName,
                                       COMPONENTS OF CommonResultsSeq,
    ...
      }},
  ...
}

-- Errors and parameters
abandoned ERROR ::= { -- not literally an "error"
  PARAMETER OPTIONALLY-PROTECTED  {SET {COMPONENTS OF CommonResults,
                                        ...}}
  CODE                            id-errcode-abandoned
}

abandonFailed ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {problem    [0]  AbandonProblem,
          operation  [1]  InvokeId,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                            id-errcode-abandonFailed
}

AbandonProblem ::= INTEGER {noSuchOperation(1), tooLate(2), cannotAbandon(3)}

attributeError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {object    [0]  Name,
          problems
            [1]  SET OF
                   SEQUENCE {problem  [0]  AttributeProblem,
                             type     [1]  AttributeType,
                             value    [2]  AttributeValue OPTIONAL,
                             ...},
          COMPONENTS OF CommonResults,
          ...}}
  CODE                            id-errcode-attributeError
}

AttributeProblem ::= INTEGER {
  noSuchAttributeOrValue(1), invalidAttributeSyntax(2),
  undefinedAttributeType(3), inappropriateMatching(4), constraintViolation(5),
  attributeOrValueAlreadyExists(6), contextViolation(7)}

nameError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {problem  [0]  NameProblem,
          matched  [1]  Name,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                            id-errcode-nameError
}

NameProblem ::= INTEGER {
  noSuchObject(1), aliasProblem(2), invalidAttributeSyntax(3),
  aliasDereferencingProblem(4), contextProblem(5)}

referral ERROR ::= { -- not literally an "error"
```

```
  PARAMETER OPTIONALLY-PROTECTED
    {SET {candidate  [0]  ContinuationReference,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                          id-errcode-referral
}

securityError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {problem   [0]  SecurityProblem,
          spkmInfo  [1]  SPKM-ERROR,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                          id-errcode-securityError
}

SecurityProblem ::= INTEGER {
  inappropriateAuthentication(1), invalidCredentials(2),
  insufficientAccessRights(3), invalidSignature(4), protectionRequired(5),
  noInformation(6),
  blockedCredentials(7),
  -- invalidQOPMatch             (8), obsolete
  spkmError(9)}

serviceError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {problem  [0]  ServiceProblem,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                          id-errcode-serviceError
}

ServiceProblem ::= INTEGER {
  busy(1), unavailable(2), unwillingToPerform(3), chainingRequired(4),
  unableToProceed(5), invalidReference(6), timeLimitExceeded(7),
  administrativeLimitExceeded(8), loopDetected(9),
  unavailableCriticalExtension(10), outOfScope(11), ditError(12),
  invalidQueryReference(13), requestedServiceNotAvailable(14),
  unsupportedMatchingUse(15), ambiguousKeyAttributes(16),
  saslBindInProgress(17)}

updateError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {problem        [0]  UpdateProblem,
          attributeInfo
            [1]  SET SIZE (1..MAX) OF
                   CHOICE {attributeType  AttributeType,
                           attribute      Attribute{{SupportedAttributes}},
                   ...
                   } OPTIONAL,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                          id-errcode-updateError
}

UpdateProblem ::= INTEGER {
  namingViolation(1), objectClassViolation(2), notAllowedOnNonLeaf(3),
  notAllowedOnRDN(4), entryAlreadyExists(5), affectsMultipleDSAs(6),
  objectClassModificationProhibited(7), noSuchSuperior(8), notAncestor(9),
  parentNotAncestor(10), hierarchyRuleViolation(11), familyRuleViolation(12)
}

-- attribute types
id-at-family-information OBJECT IDENTIFIER ::= {id-at 64}

END -- DirectoryAbstractService
```

ISO/IEC 9594-4 : 2008, Information Technology - Open systems Interconnection - The Directory: Procedures for distributed operation

Working draft for Amendment 1: Communications support enhancements

Annex A

ASN.1 for Distributed Operations

Replace the ASN.1 module in Annex A with the following

```
DistributedOperations {joint-iso-itu-t ds(5) module(1) distributedOperations(3)
  6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  basicAccessControl, commonProtocolSpecification, directoryAbstractService,
    enhancedSecurity, informationFramework, selectedAttributeTypes,
    serviceAdministration
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  DistinguishedName, Name, RDNSequence
    FROM InformationFramework informationFramework
  MRMapping, SearchRuleId
    FROM ServiceAdministration serviceAdministration
  AuthenticationLevel
    FROM BasicAccessControl basicAccessControl
  OPTIONALLY-PROTECTED{}
    FROM EnhancedSecurity enhancedSecurity
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  abandon, addEntry, CommonResults, compare, directoryBind, list, modifyDN,
    modifyEntry, read, referral, removeEntry, search, SecurityParameters
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  ERROR, id-errcode-dsaReferral, OPERATION
    FROM CommonProtocolSpecification commonProtocolSpecification
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  PresentationAddress, ProtocolInformation, UnboundedDirectoryString,
    UniqueIdentifier
    FROM SelectedAttributeTypes selectedAttributeTypes;

-- parameterized type for deriving chained operations
chained{OPERATION:operation} OPERATION ::= {
  ARGUMENT OPTIONALLY-PROTECTED
    {SET {chainedArgument  ChainingArguments,
          argument         [0]  operation.&ArgumentType}}
  RESULT OPTIONALLY-PROTECTED
    {SET {chainedResult  ChainingResults,
          result         [0]  operation.&ResultType}}
  ERRORS
    {operation.&Errors EXCEPT referral | dsaReferral}
  CODE                          operation.&operationCode
}
```

```
--  bind unbind operation
dSABind OPERATION ::= directoryBind

--  chained operations
chainedRead OPERATION ::= chained{read}

chainedCompare OPERATION ::= chained{compare}

chainedAbandon OPERATION ::= abandon

chainedList OPERATION ::= chained{list}

chainedSearch OPERATION ::= chained{search}

chainedAddEntry OPERATION ::= chained{addEntry}

chainedRemoveEntry OPERATION ::= chained{removeEntry}

chainedModifyEntry OPERATION ::= chained{modifyEntry}

chainedModifyDN OPERATION ::= chained{modifyDN}

-- errors and parameters
dsaReferral ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED
    {SET {reference      [0]  ContinuationReference,
          contextPrefix  [1]  DistinguishedName OPTIONAL,
          COMPONENTS OF CommonResults,
          ...}}
  CODE                          id-errcode-dsaReferral
}

--  common arguments and results
ChainingArguments ::= SET {
  originator              [0]  DistinguishedName OPTIONAL,
  targetObject            [1]  DistinguishedName OPTIONAL,
  operationProgress
    [2]  OperationProgress DEFAULT {nameResolutionPhase notStarted},
  traceInformation        [3]  TraceInformation,
  aliasDereferenced       [4]  BOOLEAN DEFAULT FALSE,
  aliasedRDNs             [5]  INTEGER OPTIONAL,
  -- only present in first edition systems
  returnCrossRefs         [6]  BOOLEAN DEFAULT FALSE,
  referenceType           [7]  ReferenceType DEFAULT superior,
  info                    [8]  DomainInfo OPTIONAL,
  timeLimit               [9]  Time OPTIONAL,
  securityParameters      [10]  SecurityParameters DEFAULT {},
  entryOnly               [11]  BOOLEAN DEFAULT FALSE,
  uniqueIdentifier        [12]  UniqueIdentifier OPTIONAL,
  authenticationLevel     [13]  AuthenticationLevel OPTIONAL,
  exclusions              [14]  Exclusions OPTIONAL,
  excludeShadows          [15]  BOOLEAN DEFAULT FALSE,
  nameResolveOnMaster     [16]  BOOLEAN DEFAULT FALSE,
  operationIdentifier     [17]  INTEGER OPTIONAL,
  searchRuleId            [18]  SearchRuleId OPTIONAL,
  chainedRelaxation       [19]  MRMapping OPTIONAL,
  relatedEntry            [20]  INTEGER OPTIONAL,
  dspPaging               [21]  BOOLEAN DEFAULT FALSE,
  nonDapPdu               [22]  ENUMERATED {ldap(0)} OPTIONAL,
  streamedResults         [23]  INTEGER OPTIONAL,
  excludeWriteableCopies  [24]  BOOLEAN DEFAULT FALSE,
  ...
}

Time ::= CHOICE {utcTime          UTCTime,
                 generalizedTime  GeneralizedTime,
                 ...
```

```
}

DomainInfo ::= ABSTRACT-SYNTAX.&Type

ChainingResults ::= SET {
  info                [0]  DomainInfo OPTIONAL,
  crossReferences     [1]  SEQUENCE SIZE (1..MAX) OF CrossReference OPTIONAL,
  securityParameters  [2]  SecurityParameters DEFAULT {},
  alreadySearched     [3]  Exclusions OPTIONAL,
  ...
}

CrossReference ::= SET {
  contextPrefix  [0]  DistinguishedName,
  accessPoint    [1]  AccessPointInformation,
  ...
}

OperationProgress ::= SET {
  nameResolutionPhase
    [0]  ENUMERATED {notStarted(1), proceeding(2), completed(3)},
  nextRDNToBeResolved  [1]  INTEGER OPTIONAL,
  ...
}

TraceInformation ::= SEQUENCE OF TraceItem

TraceItem ::= SET {
  dsa               [0]  Name,
  targetObject      [1]  Name OPTIONAL,
  operationProgress [2]  OperationProgress,
  ...
}

ReferenceType ::= ENUMERATED {
  superior(1), subordinate(2), cross(3), nonSpecificSubordinate(4),
  supplier(5), master(6), immediateSuperior(7), self(8), ditBridge(9),...
}

AccessPoint ::= SET {
  ae-title            [0]  Name,
  address             [1]  PresentationAddress,
  protocolInformation [2]  SET SIZE (1..MAX) OF ProtocolInformation OPTIONAL,
  labeledURI          [6]  LabeledURI OPTIONAL,
  ...
}

LabeledURI ::= UnboundedDirectoryString

MasterOrShadowAccessPoint ::= SET {
  COMPONENTS OF AccessPoint,
  category         [3]  ENUMERATED {master(0), shadow(1)} DEFAULT master,
  chainingRequired [5]  BOOLEAN DEFAULT FALSE,
  ...
}

MasterAndShadowAccessPoints ::= SET SIZE (1..MAX) OF MasterOrShadowAccessPoint

AccessPointInformation ::= SET {
  COMPONENTS OF MasterOrShadowAccessPoint,
  additionalPoints [4]  MasterAndShadowAccessPoints OPTIONAL,
  ...
}

DitBridgeKnowledge ::= SEQUENCE {
  domainLocalID  UnboundedDirectoryString OPTIONAL,
  accessPoints   MasterAndShadowAccessPoints,
  ...
```

```
}

Exclusions ::= SET SIZE (1..MAX) OF RDNSequence

ContinuationReference ::= SET {
  targetObject         [0]  Name,
  aliasedRDNs          [1]  INTEGER OPTIONAL, -- only present in first edition systems
  operationProgress    [2]  OperationProgress,
  rdnsResolved         [3]  INTEGER OPTIONAL,
  referenceType        [4]  ReferenceType,
  accessPoints         [5]  SET OF AccessPointInformation,
  entryOnly            [6]  BOOLEAN DEFAULT FALSE,
  exclusions           [7]  Exclusions OPTIONAL,
  returnToDUA          [8]  BOOLEAN DEFAULT FALSE,
  nameResolveOnMaster  [9]  BOOLEAN DEFAULT FALSE,
  ...
}

END -- DistributedOperations
```

Replace the ASN.1 module in Annex D with the following

```
HierarchicalOperationalBindings {joint-iso-itu-t ds(5) module(1)
  hierarchicalOperationalBindings(20) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryOperationalBindingTypes, directoryOSIProtocols,
    distributedOperations, informationFramework, opBindingManagement
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Attribute{}, DistinguishedName, RelativeDistinguishedName,
    SupportedAttributes
    FROM InformationFramework informationFramework
  OPERATIONAL-BINDING
    FROM OperationalBindingManagement opBindingManagement
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  MasterAndShadowAccessPoints
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  directorySystemAC
    FROM DirectoryOSIProtocols directoryOSIProtocols
  id-op-binding-hierarchical, id-op-binding-non-specific-hierarchical
    FROM DirectoryOperationalBindingTypes directoryOperationalBindingTypes;

-- types
HierarchicalAgreement ::= SEQUENCE {
  rdn                [0]  RelativeDistinguishedName,
  immediateSuperior  [1]  DistinguishedName,
  ...
}

SuperiorToSubordinate ::= SEQUENCE {
  contextPrefixInfo      [0]  DITcontext,
  entryInfo
    [1]  SET SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  immediateSuperiorInfo
    [2]  SET SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  ...
```

```
}

DITcontext ::= SEQUENCE OF Vertex

Vertex ::= SEQUENCE {
  rdn           [0]  RelativeDistinguishedName,
  admPointInfo
    [1]  SET SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  subentries    [2]  SET SIZE (1..MAX) OF SubentryInfo OPTIONAL,
  accessPoints  [3]  MasterAndShadowAccessPoints OPTIONAL,
  ...
}

SubentryInfo ::= SEQUENCE {
  rdn   [0]  RelativeDistinguishedName,
  info  [1]  SET OF Attribute{{SupportedAttributes}},
  ...
}

SubordinateToSuperior ::= SEQUENCE {
  accessPoints  [0]  MasterAndShadowAccessPoints OPTIONAL,
  alias         [1]  BOOLEAN DEFAULT FALSE,
  entryInfo
    [2]  SET SIZE (1..MAX) OF Attribute{{SupportedAttributes}} OPTIONAL,
  subentries    [3]  SET SIZE (1..MAX) OF SubentryInfo OPTIONAL,
  ...
}

SuperiorToSubordinateModification ::=
  SuperiorToSubordinate(WITH COMPONENTS {
                          ...,
                          entryInfo  ABSENT
                        })

NonSpecificHierarchicalAgreement ::= SEQUENCE {
  immediateSuperior  [1]  DistinguishedName,
  ...
}

NHOBSuperiorToSubordinate ::=
  SuperiorToSubordinate(WITH COMPONENTS {
                          ...,
                          entryInfo  ABSENT
                        })

NHOBSubordinateToSuperior ::= SEQUENCE {
  accessPoints  [0]  MasterAndShadowAccessPoints OPTIONAL,
  subentries    [3]  SET SIZE (1..MAX) OF SubentryInfo OPTIONAL,
  ...
}

-- operational binding information objects
hierarchicalOperationalBinding OPERATIONAL-BINDING ::= {
  AGREEMENT             HierarchicalAgreement
  APPLICATION CONTEXTS  {{directorySystemAC}}
  ASYMMETRIC ROLE-A
    { -- superior DSAESTABLISHMENT-INITIATOR  TRUE
                   ESTABLISHMENT-PARAMETER  SuperiorToSubordinate
                   MODIFICATION-INITIATOR   TRUE
                   MODIFICATION-PARAMETER   SuperiorToSubordinateModification
                   TERMINATION-INITIATOR    TRUE}
  ROLE-B
    { -- subordinate DSAESTABLISHMENT-INITIATOR  TRUE
                      ESTABLISHMENT-PARAMETER  SubordinateToSuperior
                      MODIFICATION-INITIATOR   TRUE
                      MODIFICATION-PARAMETER   SubordinateToSuperior
                      TERMINATION-INITIATOR    TRUE}
  ID                  id-op-binding-hierarchical
```

```
}

nonSpecificHierarchicalOperationalBinding OPERATIONAL-BINDING ::= {
  AGREEMENT             NonSpecificHierarchicalAgreement
  APPLICATION CONTEXTS  {{directorySystemAC}}
  ASYMMETRIC ROLE-A
    { -- superior DSAESTABLISHMENT-PARAMETER  NHOBSuperiorToSubordinate
                  MODIFICATION-INITIATOR   TRUE
                  MODIFICATION-PARAMETER   NHOBSuperiorToSubordinate
                  TERMINATION-INITIATOR    TRUE}
  ROLE-B
    { -- subordinate DSAESTABLISHMENT-INITIATOR  TRUE
                     ESTABLISHMENT-PARAMETER  NHOBSubordinateToSuperior
                     MODIFICATION-INITIATOR   TRUE
                     MODIFICATION-PARAMETER   NHOBSubordinateToSuperior
                     TERMINATION-INITIATOR    TRUE}
  ID                 id-op-binding-non-specific-hierarchical
}

END -- HierarchicalOperationalBindings
```

ISO/IEC 9594-5 : 2008, Information Technology - Open systems Interconnection - The Directory: Protocols

Working draft for Amendment 1: Communications support enhancements

In 7.6.1.1 item d), update the third bullet as shown:

– a **transfer-syntax-name-list**, which shall consist of one or more ~~a single~~ elements being the object identifiers for ASN.1 encoding rules as listed below~~the Basic Encoding Rules (BER)~~;

i **{joint-iso-itu-t asn1(1) basic-encoding(1)}**, which is the object identifier for the Basic Encoding Rules (BER);

ii **{joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1)}**, which is the object identifier for the Distinguished Encoding Rules (DER);

iii **{joint-iso-itu-t asn1(1) packed-encoding(3) aligned(0)}**, which is the object identifier for the Packed Encoding rules (PER), basic aligned variant--Needs discussion

iv **{joint-iso-itu-t asn1(1) packed-encoding(3) unaligned(1) }**,which is the object identifier for the Packet Encoding rules (PER), basic unaligned variant --Needs discussion

v **{joint-iso-itu-t asn1(1) xml-encoding(5) basic(0)}**, which is the object identifier for the basic XML Encoding rules (XER), --Needs discussion

~~NOTE 2 – ITU-T Rec. X.226 | ISO/IEC 8823-1 allows several transfer syntaxes to be suggested, where one of those is then elected by the responder. The extensibility rules defined in clause 12 require the use of BER.~~

In 7.6.2.1 item c), update the second bullet as shown:

– The **transfer-syntax-name** shall be present and specify the object identifier for the encoding rules elected by the responder~~Basic Encoding Rules (BER)~~.

In 7.6.3.1 item c), update the first bullet as shown:

– if the rejection is not related to presentation context negotiation, the **result** element shall be set to **acceptance**, **transfer-syntax-name** shall be present specifying the object identifier for the encoding rules elected by the responder~~Basic Encoding Rules (BER)~~, and **provider-reason** element shall be absent;

Update 9.6 as shown:

~~Each IDM-PDU is encoded using the ASN.1 Basic Encoding Rules without restriction.~~ The binary data resulting from the encoding of an IDM-PDU is then partitioned and placed in one or more segments to be sent over the TCP/IP connection. Each segment has a *header* and carries the next *fragment* or portion of the encoded data. The division of an IDM-PDU into fragments and the size of any fragment are at the choice of the sender and carry no significance. All fragments of an IDM-PDU shall be sent before another IDM-PDU is sent.

The format of a segment is determined by the version of the segment. New versions are introduced as additional information is required in the header. The first octet of is the `version` field.

The version number shall be the same for all IDM-PDUs within an application-association. If a request or response is received violating this rule, the receiver shall return an **`IdmReject`** with reason code **`invalideIdmVersion`**. This reject shall be transferred using the version agreed for the application-association.

If the version field indicates an unsupported version, the receiving DSA shall return an **`IdmReject`** with reason code **`unsupportedIdmVersion`**. This reject shall be transferred using a version 1 format.

An implementation shall support the version 1 format in the response to an **`IdmBind`**.

A DSA may also reject an **`IdmBind`** if existing application-associations are using a version different from the one suggested in the format suggested by the **`IdmBind`**. In this case, an **`IdmReject`** with reason code **`unsuitableIdmVersion`** shall be returned. This reject shall be transferred using the same version as used for the request.

The format for a version 1 segment (header plus fragment of an IDM-PDU) is as follows:

version (1 octet)	final (1 octet)	length (4 octets)	data (*length* octets)

For version 1, each IDM-PDU is encoded using the ASN.1 Basic Encoding Rules without restriction.

The format for a version 2 segment is as follows:

version (1 octet)	final (1 octet)	encoding (2 octets)	length (4 octets)	data (*length* octets)

`final` indicates whether `data` holds a non-final IDM-PDU fragment (value 0), or the whole value or final fragment (value 1).

`encoding` indicates which transfer syntax(es) other than Basic Encoding Rules (BER) are supported. This fields is considered as a bit string containing 16 bits defined as follows:

i. bit 1: Distinguished Encoding Rules (DER);

ii. bit 2: Packed Encoding Rules (PER), basic aligned variant;

iii. bit 3: Packed Encoding Rules (PER), basic unaligned variant;

iv. bit 4: XML Encoding Rules (XER).

The other bits are reserved for future use.

The **`encoding`** field of **`IdmBind`** request specifies all the supported encoding rules. In the **`IdmBind`** response, at most one of the bits set in the **`IdmBind`** request can be set. If the **`encoding`** field of the **`IdmBind`** response is not zero, the corresponding encoding rules shall be used; else Basic Encoding Rules shall be used. The **`encoding`** field is not used in other PDUs and shall contain zero.

More text here

`length` is the length of `data` field in octets. It is sent in 'network octet order' with more significant octets preceding less significant octets. The minimum value of length is 1. For performance reasons, it is recommended that the whole IDM-PDU be contained in one segment if the length can be expressed in the 4 octets of the length field; IDM fragmentation should only be used if the length of the IDM-PDU cannot be expressed in 4 octets.

`data` holds the next fragment of the IDM-PDU being conveyed, or the whole IDM-PDU if the whole value is conveyed in one fragment.

Annex A

Common protocol specifications in ASN.1

Replace the ASN.1 module in Annex A with the following

```
CommonProtocolSpecification {joint-iso-itu-t ds(5) module(1)
  commonProtocolSpecification(35) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the
-- other ASN.1 modules contained within the Directory Specifications, and for
-- the use of other applications which will use them to access Directory
-- services. Other applications may use them for their own purposes, but this
-- will not constrain extensions and modifications needed to maintain or
-- improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  opBindingManagement
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  establishOperationalBinding, modifyOperationalBinding,
    terminateOperationalBinding
    FROM OperationalBindingManagement opBindingManagement;

OPERATION ::= CLASS {
  &ArgumentType   OPTIONAL,
  &ResultType     OPTIONAL,
  &Errors         ERROR OPTIONAL,
  &operationCode  Code UNIQUE OPTIONAL
}
WITH SYNTAX {
  [ARGUMENT &ArgumentType]
  [RESULT &ResultType]
  [ERRORS &Errors]
  [CODE &operationCode]
}

ERROR ::= CLASS {&ParameterType  ,
                 &errorCode      Code UNIQUE OPTIONAL
}WITH SYNTAX {PARAMETER &ParameterType
              [CODE &errorCode]
}

Code ::= CHOICE {local   INTEGER,
                 global  OBJECT IDENTIFIER,
                 ...
}

InvokeId ::= CHOICE {present  INTEGER,
                     absent   NULL,
                     ...
}

--  operation codes for DAP and DSP
id-opcode-read Code ::= local:1

id-opcode-compare Code ::= local:2

id-opcode-abandon Code ::= local:3

id-opcode-list Code ::= local:4

id-opcode-search Code ::= local:5

id-opcode-addEntry Code ::= local:6
```

```
id-opcode-removeEntry Code ::= local:7

id-opcode-modifyEntry Code ::= local:8

id-opcode-modifyDN Code ::= local:9

--  operation codes for DISP
id-opcode-requestShadowUpdate Code ::= local:1

id-opcode-updateShadow Code ::= local:2

id-opcode-coordinateShadowUpdate Code ::= local:3

--  operation codes for DOP
id-op-establishOperationalBinding Code ::= local:100

id-op-modifyOperationalBinding Code ::= local:102

id-op-terminateOperationalBinding Code ::= local:101

-- error codes for DAP and DSP
id-errcode-attributeError Code ::= local:1

id-errcode-nameError Code ::= local:2

id-errcode-serviceError Code ::= local:3

id-errcode-referral Code ::= local:4

id-errcode-abandoned Code ::= local:5

id-errcode-securityError Code ::= local:6

id-errcode-abandonFailed Code ::= local:7

id-errcode-updateError Code ::= local:8

id-errcode-dsaReferral Code ::= local:9

-- error code for DISP
id-errcode-shadowError Code ::= local:1

-- error code for DOP
id-err-operationalBindingError Code ::= local:100

DOP-Invokable OPERATION ::=
  {establishOperationalBinding | modifyOperationalBinding |
   terminateOperationalBinding}

DOP-Returnable OPERATION ::=
  {establishOperationalBinding | modifyOperationalBinding |
   terminateOperationalBinding}

END -- CommonProtocolSpecification
```

Annex B

OSI Protocol in ASN.1

Replace the ASN.1 module in Annex B with the following

```
OSIProtocolSpecification {joint-iso-itu-t ds(5) module(1)
  oSIProtocolSpecification(36) 6} DEFINITIONS ::=
```

```
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access Directory
-- services. Other applications may use them for their own purposes, but this will not
constrain extensions
-- and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  commonProtocolSpecification, directoryAbstractService, directoryOSIProtocols,
    enhancedSecurity, informationFramework
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Name, RelativeDistinguishedName
    FROM InformationFramework informationFramework
  OPTIONALLY-PROTECTED
    FROM EnhancedSecurity enhancedSecurity
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  SecurityProblem, ServiceProblem, Versions
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  InvokeId, OPERATION
    FROM CommonProtocolSpecification commonProtocolSpecification
  APPLICATION-CONTEXT
    FROM DirectoryOSIProtocols directoryOSIProtocols;

-- OSI protocol
OSI-PDU{APPLICATION-CONTEXT:protocol} ::=
  TYPE-IDENTIFIER.&Type
    (OsiBind{{protocol}} | OsiBindResult{{protocol}} | OsiBindError{{protocol}}
     | OsiOperation{{protocol.&Operations}} | PresentationAbort)

OsiBind{APPLICATION-CONTEXT:Protocols} ::= SET {
  mode-selector           [0] IMPLICIT SET {mode-value  [0] IMPLICIT INTEGER(1)
  },
  normal-mode-parameters
    [2] IMPLICIT SEQUENCE {protocol-version
                             [0] IMPLICIT BIT STRING {version-1(0)}
                               DEFAULT {version-1},
                           calling-presentation-selector
                             [1] IMPLICIT Presentation-selector OPTIONAL,
                           called-presentation-selector
                             [2] IMPLICIT Presentation-selector OPTIONAL,
                           presentation-context-definition-list
                             [4] IMPLICIT Context-list,
                           user-data
                             CHOICE {fully-encoded-data
                                       [APPLICATION 1] IMPLICIT SEQUENCE
                                                         SIZE (1) OF
                                                         SEQUENCE {transfer-
syntax-name
                                                           Transfer-syntax-name
                                                           OPTIONAL,
                                                         presentation-context-
identifier
                                                           Presentation-context-
identifier,
                                                         presentation-data-
values
                                                           CHOICE {single-ASN1-
type
```

```
                                                              [0]  AARQ-apdu
                                                              {
                                                              {Protocols}}
                                                              }
                                                            }}}
}

Presentation-selector ::= OCTET STRING(SIZE (1..4, ..., 5..MAX))

Context-list ::=
  SEQUENCE SIZE (2) OF
    SEQUENCE {presentation-context-identifier  Presentation-context-identifier,
              abstract-syntax-name             Abstract-syntax-name,
              transfer-syntax-name-list        SEQUENCE OF Transfer-syntax-name
    }

Presentation-context-identifier ::= INTEGER(1..127, ..., 128..MAX)

Abstract-syntax-name ::= OBJECT IDENTIFIER

Transfer-syntax-name ::= OBJECT IDENTIFIER

AARQ-apdu{APPLICATION-CONTEXT:Protocols} ::=
  [APPLICATION 0] IMPLICIT SEQUENCE {
  protocol-version
    [0] IMPLICIT BIT STRING {version1(0)} DEFAULT {version1},
  application-context-name          [1]  Application-context-name,
  called-AP-title                   [2]  Name OPTIONAL,
  called-AE-qualifier               [3]  RelativeDistinguishedName OPTIONAL,
  called-AP-invocation-identifier   [4]  AP-invocation-identifier OPTIONAL,
  called-AE-invocation-identifier   [5]  AE-invocation-identifier OPTIONAL,
  calling-AP-title                  [6]  Name OPTIONAL,
  calling-AE-qualifier              [7]  RelativeDistinguishedName OPTIONAL,
  calling-AP-invocation-identifier  [8]  AP-invocation-identifier OPTIONAL,
  calling-AE-invocation-identifier  [9]  AE-invocation-identifier OPTIONAL,
  implementation-information        [29] IMPLICIT Implementation-data OPTIONAL,
  user-information
    [30] IMPLICIT Association-informationBind{{Protocols}}
}

Association-informationBind{APPLICATION-CONTEXT:Protocols} ::=
  SEQUENCE SIZE (1) OF
    EXTERNAL
      (WITH COMPONENTS {
         identification         (WITH COMPONENTS {
                                   syntax  ABSENT
                                 }),
         data-value-descriptor  ABSENT,
         data-value             (CONTAINING TheOsiBind{{Protocols}})
       })

Application-context-name ::= OBJECT IDENTIFIER

AP-invocation-identifier ::= INTEGER

AE-invocation-identifier ::= INTEGER

Implementation-data ::= GraphicString

TheOsiBind{APPLICATION-CONTEXT:Protocols} ::=
  [16]  APPLICATION-CONTEXT.&bind-operation.&ArgumentType({Protocols})

OsiBindResult{APPLICATION-CONTEXT:Protocols} ::= SET {
  mode-selector          [0] IMPLICIT SET {mode-value  [0] IMPLICIT INTEGER(1)},
  normal-modeparameters
    [2] IMPLICIT SEQUENCE {protocol-version
                             [0] IMPLICIT BIT STRING {version-1(0)}
                               DEFAULT {version-1},
```

```
                          responding-presentation-selector
                            [3] IMPLICIT Presentation-selector OPTIONAL,
                          presentation-context-definition-result-list
                            [5] IMPLICIT SEQUENCE SIZE (2) OF
                                         SEQUENCE {result
                                                     [0] IMPLICIT Result
                                                                  (acceptance),
                                                   transfer-syntax-name
                                                     [1] IMPLICIT Transfer-syntax-name
                                         },
                          user-data
                            CHOICE {fully-encoded-data
                                      [APPLICATION 1] IMPLICIT SEQUENCE
                                                               SIZE (1) OF
                                                               SEQUENCE {transfer-
syntax-name

                                                                 Transfer-syntax-name
                                                                 OPTIONAL,
                                                                 presentation-context-
identifier

                                                                 Presentation-context-
identifier,
                                                                 presentation-data-
values

                                                                 CHOICE {single-ASN1-
type

                                                                 [0]  AARE-apdu
                                                                 {
                                                                 {Protocols}}
                                                                 }
                                                               }}}
}

Result ::= INTEGER {acceptance(0), user-rejection(1), provider-rejection(2)}

AARE-apdu{APPLICATION-CONTEXT:Protocols} ::=
  [APPLICATION 1] IMPLICIT SEQUENCE {
  protocol-version
    [0] IMPLICIT BIT STRING {version1(0)} DEFAULT {version1},
  application-context-name             [1]  Application-context-name,
  result                               [2]  Associate-result(accepted),
  result-source-diagnostic             [3]  Associate-source-diagnostic,
  responding-AP-title                  [4]  Name OPTIONAL,
  responding-AE-qualifier              [5]  RelativeDistinguishedName OPTIONAL,
  responding-AP-invocation-identifier  [6]  AP-invocation-identifier OPTIONAL,
  responding-AE-invocation-identifier  [7]  AE-invocation-identifier OPTIONAL,
  implementation-information
    [29] IMPLICIT Implementation-data OPTIONAL,
  user-information
    [30] IMPLICIT Association-informationBindRes{{Protocols}}
}

Association-informationBindRes{APPLICATION-CONTEXT:Protocols} ::=
  SEQUENCE SIZE (1) OF
    EXTERNAL
      (WITH COMPONENTS {
         identification         (WITH COMPONENTS {
                                   syntax  ABSENT
                                 }),
         data-value-descriptor  ABSENT,
         data-value             (CONTAINING TheOsiBindRes{{Protocols}})
       })

Associate-result ::= INTEGER {
```

```
  accepted(0), rejected-permanent(1), rejected-transient(2)}(0..2, ...)

Associate-source-diagnostic ::= CHOICE {
  acse-service-user
    [1]  INTEGER {null(0), no-reason-give(1),
                  application-context-name-not-supported(2),
                  calling-AP-title-not-recognized(3),
                  calling-AP-invocation-identifier-not-recognized(4),
                  calling-AE-qualifier-not-recognized(5),
                  calling-AE-invocation-identifier-not-recognized(6),
                  called-AP-title-not-recognized(7),
                  called-AP-invocation-identifier-not-recognized(8),
                  called-AE-qualifier-not-recognized(9),
                  called-AE-invocation-identifier-not-recognized(10)}
                                                                  (0..10, ...),
  acse-service-provider
    [2]  INTEGER {null(0), no-reason-given(1), no-common-acse-version(2)}
                                                                  (0..2, ...)
}

TheOsiBindRes{APPLICATION-CONTEXT:Protocols} ::=
  [17]  APPLICATION-CONTEXT.&bind-operation.&ResultType({Protocols})

OsiBindError{APPLICATION-CONTEXT:Protocols} ::= CHOICE {
  normal-mode-parameters
    SEQUENCE {protocol-version
                [0] IMPLICIT BIT STRING {version-1(0)} DEFAULT {version-1},
              responding-presentation-selector
                [3] IMPLICIT Presentation-selector OPTIONAL,
              presentation-context-definition-result-list
                [5] IMPLICIT Result-list OPTIONAL,
              provider-reason
                [10] IMPLICIT Provider-reason OPTIONAL,
              user-data
                CHOICE {fully-encoded-data
                          [APPLICATION 1] IMPLICIT SEQUENCE SIZE (1) OF
                                                    SEQUENCE {transfer-syntax-name

                                                              Transfer-syntax-name
                                                                OPTIONAL,
                                                            presentation-context-
identifier

                                                              Presentation-context-
identifier,
                                                            presentation-data-values

                                                              CHOICE {single-ASN1-type

                                                                 [0]  AAREerr-apdu
                                                                 {
                                                                 {Protocols}}
                                                            }}} OPTIONAL
  }
}

Result-list ::=
  SEQUENCE SIZE (2) OF
    SEQUENCE {result                [0] IMPLICIT Result,
              transfer-syntax-name  [1] IMPLICIT Transfer-syntax-name OPTIONAL,
              provider-reason
                [2] IMPLICIT INTEGER {reason-not-specified(0),
                                      abstract-syntax-not-supported(1),
                                      proposed-transfer-syntaxes-not-supported(2)}
                  OPTIONAL}

Provider-reason ::= INTEGER {
  reason-not-specified(0), temporary-congestion(1), local-limit-exceeded(2),
```

```
  called-presentation-address-unknown(3), protocol-version-not-supported(4),
  default-context-not-supported(5), user-data-not-readable(6),
  no-PSAP-available(7)}

AAREerr-apdu{APPLICATION-CONTEXT:Protocols} ::=
  [APPLICATION 1] IMPLICIT SEQUENCE {
  protocol-version
    [0] IMPLICIT BIT STRING {version1(0)} DEFAULT {version1},
  application-context-name             [1]  Application-context-name,
  result
    [2]  Associate-result(rejected-permanent..rejected-transient),
  result-source-diagnostic             [3]  Associate-source-diagnostic,
  responding-AP-title                  [4]  Name OPTIONAL,
  responding-AE-qualifier              [5]  RelativeDistinguishedName OPTIONAL,
  responding-AP-invocation-identifier  [6]  AP-invocation-identifier OPTIONAL,
  responding-AE-invocation-identifier  [7]  AE-invocation-identifier OPTIONAL,
  implementation-information
    [29] IMPLICIT Implementation-data OPTIONAL,
  user-information
    [30] IMPLICIT Association-informationBindErr{{Protocols}} OPTIONAL
}

Association-informationBindErr{APPLICATION-CONTEXT:Protocols} ::=
  SEQUENCE SIZE (1) OF
    EXTERNAL
      (WITH COMPONENTS {
         identification         (WITH COMPONENTS {
                                   syntax  ABSENT
                                 }),
         data-value-descriptor  ABSENT,
         data-value             (CONTAINING TheOsiBindErr{{Protocols}})
       })

TheOsiBindErr{APPLICATION-CONTEXT:Protocols} ::=
  [18]  APPLICATION-CONTEXT.&bind-operation.&Errors.&ParameterType
    ({Protocols})

OsiUnbind ::= CHOICE {
  fully-encoded-data
    [APPLICATION 1] IMPLICIT SEQUENCE SIZE (1) OF
                              SEQUENCE {presentation-context-identifier
                                          Presentation-context-identifier,
                                        presentation-data-values
                                          CHOICE {single-ASN1-type
                                                    [0]  TheOsiUnbind
                                        }}
}

TheOsiUnbind ::= [APPLICATION 2] IMPLICIT SEQUENCE {
  reason  [0] IMPLICIT Release-request-reason OPTIONAL
}

Release-request-reason ::= INTEGER {normal(0)}

OsiUnbindResult ::= CHOICE {
  fully-encoded-data
    [APPLICATION 1] IMPLICIT SEQUENCE SIZE (1) OF
                              SEQUENCE {presentation-context-identifier
                                          Presentation-context-identifier,
                                        presentation-data-values
                                          CHOICE {single-ASN1-type
                                                    [0]  TheOsiUnbindRes
                                        }}
}

TheOsiUnbindRes ::= [APPLICATION 3] IMPLICIT SEQUENCE {
  reason  [0] IMPLICIT Release-response-reason OPTIONAL
}
```

```
Release-response-reason ::= INTEGER {normal(0)}

OsiOperation{OPERATION:Operations} ::= CHOICE {
  fully-encoded-data
    [APPLICATION 1] IMPLICIT SEQUENCE SIZE (1) OF
                              SEQUENCE {presentation-context-identifier
                                          Presentation-context-identifier,
                                        presentation-data-values
                                          CHOICE {single-ASN1-type
                                                    [0]  CHOICE {request
                                                                   OsiReq
                                                                   {
                                                                   {Operations}},
                                                                 result
                                                                   OsiRes
                                                                   {
                                                                   {Operations}},
                                                                 error
                                                                   OsiErr
                                                                   {
                                                                   {Operations}},
                                                                 reject
                                                                   OsiRej
                                                  }}}
}

OsiReq{OPERATION:Operations} ::= [1] IMPLICIT SEQUENCE {
  invokeId  InvokeId,
  opcode    OPERATION.&operationCode({Operations}),
  argument  OPERATION.&ArgumentType({Operations}{@opcode})
}

OsiRes{OPERATION:Operations} ::= [2] IMPLICIT SEQUENCE {
  invokeId  InvokeId,
  result
    SEQUENCE {opcode  OPERATION.&operationCode({Operations}),
              result  OPERATION.&ResultType({Operations}{@.opcode})
  }
}

OsiErr{OPERATION:Operations} ::= [3] IMPLICIT SEQUENCE {
  invokeID  InvokeId,
  errcode   OPERATION.&Errors.&errorCode({Operations}),
  error     OPERATION.&Errors.&ParameterType({Operations}{@.errcode})
}

OsiRej ::= [4] IMPLICIT SEQUENCE {
  invokeId  InvokeId,
  problem
    CHOICE {general       [0]  GeneralProblem,
            invoke        [1]  InvokeProblem,
            returnResult  [2]  ReturnResultProblem,
            returnError   [3]  ReturnErrorProblem}
}

GeneralProblem ::= INTEGER {
  unrecognizedPDU(0), mistypedPDU(1), badlyStructuredPDU(2)}

InvokeProblem ::= INTEGER {
  duplicateInvocation(0), unrecognizedOperation(1), mistypedArgument(2),
  resourceLimitation(3), releaseInProgress(4)}

ReturnResultProblem ::= INTEGER {
  unrecognizedInvocation(0), resultResponseUnexpected(1), mistypedResult(2)
}

ReturnErrorProblem ::= INTEGER {
```

```
  unrecognizedInvocation(0), errorResponseUnexpected(1), unrecognizedError(2),
  unexpectedError(3), mistypedParameter(4)}

PresentationAbort ::= CHOICE {aru-ppdu  ARU-PPDU,
                              arp-ppdu  ARP-PPDU
}

ARU-PPDU ::= CHOICE {
  normal-mode-parameters
    [0] IMPLICIT SEQUENCE {presentation-context-identifier-list
                             [0] IMPLICIT Presentation-context-identifier-list,
                           user-data
                             CHOICE {fully-encoded-data
                                       [APPLICATION 1] IMPLICIT SEQUENCE
                                                                 SIZE (1) OF
                                                                 SEQUENCE {presentation-
context-identifier

                                                                   Presentation-context-
identifier,
                                                                   presentation-data-
values

                                                                   CHOICE {single-ASN1-
type

                                                                   [0]  ABRT-apdu
                                                                   }
                                                                 }}}
}

Presentation-context-identifier-list ::=
  SEQUENCE SIZE (1) OF
    SEQUENCE {presentation-context-identifier  Presentation-context-identifier,
              transfer-syntax-name             Transfer-syntax-name}

ABRT-apdu ::= [APPLICATION 4] IMPLICIT SEQUENCE {abort-source  ABRT-source
}

ABRT-source ::= INTEGER {acse-service-user(0), acse-service-provider(1)}

ARP-PPDU ::= SEQUENCE {
  provider-reason   [0] IMPLICIT Abort-reason OPTIONAL,
  event-identifier  [1] IMPLICIT Event-identifier OPTIONAL
}

Abort-reason ::= INTEGER {
  reason-not-specified(0), unrecognized-ppdu(1), unexpected-ppdu(2),
  unexpected-session-service-primitive(3), unrecognized-ppdu-parameter(4),
  unexpected-ppdu-parameter(5), invalid-ppdu-parameter-value(6)}

Event-identifier ::= INTEGER {
  cp-PPDU(0), cpa-PPDU(1), cpr-PPDU(2), aru-PPDU(3), arp-PPDU(4), td-PPDU(7),
  s-release-indication(14), s-release-confirm(15)}

END --OSIProtocolSpecification
```

Annex C

Directory OSI Protocols in ASN.1

Replace the ASN.1 module in Annex C with the following

```
DirectoryOSIProtocols {joint-iso-itu-t ds(5) module(1)
  directoryOSIProtocols(37) 6} DEFINITIONS ::=
```

```
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  commonProtocolSpecification, directoryAbstractService, distributedOperations,
    directoryShadowAbstractService, id-ac, id-as, id-idm,
    iDMProtocolSpecification, opBindingManagement, oSIProtocolSpecification
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  dSAOperationalBindingManagementBind, establishOperationalBinding,
    modifyOperationalBinding, terminateOperationalBinding
    FROM OperationalBindingManagement opBindingManagement
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  abandon, addEntry, compare, directoryBind, list, modifyDN, modifyEntry,
    read, removeEntry, search
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  chainedAbandon, chainedAddEntry, chainedCompare, chainedList,
    chainedModifyDN, chainedModifyEntry, chainedRead, chainedRemoveEntry,
    chainedSearch, dSABind
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  OPERATION
    FROM CommonProtocolSpecification commonProtocolSpecification
  OSI-PDU{}
    FROM OSIProtocolSpecification oSIProtocolSpecification
  -- from ITU-T Rec. X.525 | ISO/IEC 9594-9
  coordinateShadowUpdate, dSAShadowBind, requestShadowUpdate, updateShadow
    FROM DirectoryShadowAbstractService directoryShadowAbstractService;

-- OSI protocols
DAP-OSI-PDUs ::= OSI-PDU{directoryAccessAC}

DSP-OSI-PDUs ::= OSI-PDU{directorySystemAC}

DOP-OSI-PDUs ::= OSI-PDU{directoryOperationalBindingManagementAC}

ShadowSupplierInitiatedDISP-OSI-PDUs ::= OSI-PDU{shadowSupplierInitiatedAC}

ShadowSupplierInitiatedAsynchronousDISP-OSI-PDUs ::=
  OSI-PDU{shadowSupplierInitiatedAsynchronousAC}

ShadowConsumerInitiatedDISP-OSI-PDUs ::= OSI-PDU{shadowConsumerInitiatedAC}

ShadowConsumerInitiatedAsynchronousDISP-OSI-PDUs ::=
  OSI-PDU{shadowConsumerInitiatedAsynchronousAC}

APPLICATION-CONTEXT ::= CLASS {
  &bind-operation          OPERATION,
  &Operations              OPERATION,
  &applicationContextName  OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  BIND-OPERATION &bind-operation
  OPERATIONS &Operations
  APPLICATION CONTEXT NAME &applicationContextName
}

directoryAccessAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            directoryBind
```

```
  OPERATIONS
    {read | compare | abandon | list | search | addEntry | removeEntry |
      modifyEntry | modifyDN}
  APPLICATION CONTEXT NAME  id-ac-directoryAccessAC
}

directorySystemAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSABind
  OPERATIONS
    {chainedRead | chainedCompare | chainedAbandon | chainedList |
      chainedSearch | chainedAddEntry | chainedRemoveEntry | chainedModifyEntry
      | chainedModifyDN}
  APPLICATION CONTEXT NAME  id-ac-directorySystemAC
}

shadowSupplierInitiatedAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSAShadowBind
  OPERATIONS                {updateShadow | coordinateShadowUpdate}
  APPLICATION CONTEXT NAME  id-ac-shadowSupplierInitiatedAC
}

shadowConsumerInitiatedAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSAShadowBind
  OPERATIONS                {requestShadowUpdate | updateShadow}
  APPLICATION CONTEXT NAME  id-ac-shadowConsumerInitiatedAC
}

shadowSupplierInitiatedAsynchronousAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSAShadowBind
  OPERATIONS                {updateShadow | coordinateShadowUpdate}
  APPLICATION CONTEXT NAME  id-ac-shadowSupplierInitiatedAsynchronousAC
}

shadowConsumerInitiatedAsynchronousAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSAShadowBind
  OPERATIONS                {requestShadowUpdate | updateShadow}
  APPLICATION CONTEXT NAME  id-ac-shadowConsumerInitiatedAsynchronousAC
}

directoryOperationalBindingManagementAC APPLICATION-CONTEXT ::= {
  BIND-OPERATION            dSAOperationalBindingManagementBind
  OPERATIONS
    {establishOperationalBinding | modifyOperationalBinding |
      terminateOperationalBinding}
  APPLICATION CONTEXT NAME  id-ac-directoryOperationalBindingManagementAC
}

--  abstract syntaxes
id-as-directoryAccessAS OBJECT IDENTIFIER ::= {id-as 1}

id-as-directorySystemAS OBJECT IDENTIFIER ::= {id-as 2}

id-as-directoryShadowAS OBJECT IDENTIFIER ::= {id-as 3}

id-as-directoryOperationalBindingManagementAS OBJECT IDENTIFIER ::= {id-as 4}

-- id-as-directoryReliableShadowAS                          OBJECT IDENTIFIER  ::=
     {id-as 5}
-- id-as-reliableShadowBindingAS                         OBJECT IDENTIFIER  ::=  {id-as
6}
-- id-as-2or3se                                          OBJECT IDENTIFIER  ::=  {id-as
7}
id-acseAS OBJECT IDENTIFIER ::=
  {joint-iso-itu-t association-control(2) abstract-syntax(1) apdus(0)
   version(1)}

-- application context object identifiers
id-ac-directoryAccessAC OBJECT IDENTIFIER ::=
```

```
  {id-ac 1}

id-ac-directorySystemAC OBJECT IDENTIFIER ::= {id-ac 2}

id-ac-directoryOperationalBindingManagementAC OBJECT IDENTIFIER ::= {id-ac 3}

id-ac-shadowConsumerInitiatedAC OBJECT IDENTIFIER ::= {id-ac 4}

id-ac-shadowSupplierInitiatedAC OBJECT IDENTIFIER ::= {id-ac 5}

-- id-ac-reliableShadowSupplierInitiatedAC                  OBJECT IDENTIFIER  ::=
     {id-ac 6}
-- id-ac-reliableShadowConsumerInitiatedAC                  OBJECT IDENTIFIER  ::=
     {id-ac 7}
id-ac-shadowSupplierInitiatedAsynchronousAC OBJECT IDENTIFIER ::=
  {id-ac 8}

id-ac-shadowConsumerInitiatedAsynchronousAC OBJECT IDENTIFIER ::= {id-ac 9}

-- id-ac-directoryAccessWith2or3seAC                        OBJECT IDENTIFIER  ::=
     {id-ac 10}
-- id-ac-directorySystemWith2or3seAC                    OBJECT IDENTIFIER  ::=  {id-ac
11}
-- id-ac-shadowSupplierInitiatedWith2or3seAC                OBJECT IDENTIFIER  ::=
     {id-ac 12}
-- id-ac-shadowConsumerInitiatedWith2or3seAC                OBJECT IDENTIFIER  ::=
     {id-ac 13}
-- id-ac-reliableShadowSupplierInitiatedWith2or3seAC            OBJECT IDENTIFIER
     ::=  {id-ac 14}
-- id-ac-reliableShadowConsumerInitiatedWith2or3seAC            OBJECT IDENTIFIER
     ::=  {id-ac 15}
-- id-ac-directoryOperationalBindingManagementWith2or3seAC  OBJECT IDENTIFIER  ::=
     {id-ac 16}
END -- DirectoryOSIProtocols
```

Annex D

IDM Protocol in ASN.1

Replace the ASN.1 module in Annex D with the following

```
IDMProtocolSpecification {joint-iso-itu-t ds(5) module(1)
  iDMProtocolSpecification(30) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access Directory
-- services. Other applications may use them for their own purposes, but this will not
constrain extensions
-- and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  certificateExtensions, commonProtocolSpecification, directoryAbstractService,
    directoryIDMProtocols, enhancedSecurity
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  -- from ITU-T Rec. X.509 | ISO/IEC 9594-8
  GeneralName
    FROM CertificateExtensions certificateExtensions
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  SecurityProblem, ServiceProblem, Versions
    FROM DirectoryAbstractService directoryAbstractService
```

```
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  InvokeId, OPERATION
    FROM CommonProtocolSpecification commonProtocolSpecification;

-- IDM protocol
IDM-PDU{IDM-PROTOCOL:protocol} ::= CHOICE {
  bind         [0]  IdmBind{{protocol}},
  bindResult   [1]  IdmBindResult{{protocol}},
  bindError    [2]  IdmBindError{{protocol}},
  request      [3]  Request{{protocol.&Operations}},
  result       [4]  IdmResult{{protocol.&Operations}},
  error        [5]  Error{{protocol.&Operations}},
  reject       [6]  IdmReject,
  unbind       [7]  Unbind,
  abort        [8]  Abort,
  startTLS     [9]  StartTLS,
  tLSResponse  [10]  TLSResponse,
  ...
}

IdmBind{IDM-PROTOCOL:Protocols} ::= SEQUENCE {
  protocolID      IDM-PROTOCOL.&id({Protocols}),
  callingAETitle  [0]  GeneralName OPTIONAL,
  calledAETitle   [1]  GeneralName OPTIONAL,
  argument
    [2]  IDM-PROTOCOL.&bind-operation.&ArgumentType
           ({Protocols}{@protocolID}),
  ...
}

IdmBindResult{IDM-PROTOCOL:Protocols} ::= SEQUENCE {
  protocolID         IDM-PROTOCOL.&id({Protocols}),
  respondingAETitle  [0]  GeneralName OPTIONAL,
  result
    [1]  IDM-PROTOCOL.&bind-operation.&ResultType
           ({Protocols}{@protocolID}),
  ...
}

IdmBindError{IDM-PROTOCOL:Protocols} ::= SEQUENCE {
  protocolID         IDM-PROTOCOL.&id({Protocols}),
  errcode
    IDM-PROTOCOL.&bind-operation.&Errors.&errorCode
      ({Protocols}{@protocolID}),
  respondingAETitle  [0]  GeneralName OPTIONAL,
  aETitleError
    ENUMERATED {callingAETitleNotAccepted(0), calledAETitleNotRecognized(1),...}
      OPTIONAL,
  error
    [1]  IDM-PROTOCOL.&bind-operation.&Errors.&ParameterType
           ({Protocols}{@protocolID, @errcode}),
  ...
}

Request{OPERATION:Operations} ::= SEQUENCE {
  invokeID  INTEGER,
  opcode    OPERATION.&operationCode({Operations}),
  argument  OPERATION.&ArgumentType({Operations}{@opcode}),
  ...
}

IdmResult{OPERATION:Operations} ::= SEQUENCE {
  invokeID  InvokeId,
  opcode    OPERATION.&operationCode({Operations}),
  result    OPERATION.&ResultType({Operations}{@opcode}),
  ...
}
```

```
Error{OPERATION:Operations} ::= SEQUENCE {
  invokeID  INTEGER,
  errcode   OPERATION.&Errors.&errorCode({Operations}),
  error     OPERATION.&Errors.&ParameterType({Operations}{@errcode}),
  ...
}

IdmReject ::= SEQUENCE {
  invokeID  INTEGER,
  reason
    ENUMERATED {mistypedPDU(0), duplicateInvokeIDRequest(1),
                unsupportedOperationRequest(2), unknownOperationRequest(3),
                mistypedArgumentRequest(4), resourceLimitationRequest(5),
                unknownInvokeIDResult(6), mistypedResultRequest(7),
                unknownInvokeIDError(8), unknownError(9),
                mistypedParameterError(10),...},
  ...
}

Unbind ::= NULL

Abort ::= ENUMERATED {
  mistypedPDU(0), unboundRequest(1), invalidPDU(2), resourceLimitation(3),
  connectionFailed(4), invalidProtocol(5), reasonNotSpecified(6),...}

StartTLS ::= NULL

TLSResponse ::= ENUMERATED {
  success(0), operationsError(1), protocolError(2), unavailable(3),...}

-- IDM-protocol information object class
IDM-PROTOCOL ::= CLASS {
  &bind-operation  OPERATION,
  &Operations      OPERATION,
  &id              OBJECT IDENTIFIER UNIQUE
}
WITH SYNTAX {
  BIND-OPERATION &bind-operation
  OPERATIONS &Operations
  ID &id
}

END
```

Annex E

Directory IDM Protocols in ASN.1

Replace the ASN.1 module in Annex E with the following

```
DirectoryIDMProtocols {joint-iso-itu-t ds(5) module(1)
  directoryIDMProtocols(31) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryAbstractService, distributedOperations,
```

```
    directoryShadowAbstractService, id-idm, iDMProtocolSpecification,
    opBindingManagement
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  establishOperationalBinding, modifyOperationalBinding,
    terminateOperationalBinding
    FROM OperationalBindingManagement opBindingManagement
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  abandon, addEntry, compare, directoryBind, list, modifyDN, modifyEntry,
    read, removeEntry, search
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  chainedAbandon, chainedAddEntry, chainedCompare, chainedList,
    chainedModifyDN, chainedModifyEntry, chainedRead, chainedRemoveEntry,
    chainedSearch
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  IDM-PDU, IDM-PROTOCOL
    FROM IDMProtocolSpecification iDMProtocolSpecification
  -- from ITU-T Rec. X.525 | ISO/IEC 9594-9
  coordinateShadowUpdate, requestShadowUpdate, updateShadow
    FROM DirectoryShadowAbstractService directoryShadowAbstractService;

-- IDM protocols
DAP-IDM-PDUs ::= IDM-PDU{dap-ip}

dap-ip IDM-PROTOCOL ::= {
  BIND-OPERATION  directoryBind
  OPERATIONS
    {read | compare | abandon | list | search | addEntry | removeEntry |
      modifyEntry | modifyDN}
  ID              id-idm-dap
}

DSP-IDM-PDUs ::= IDM-PDU{dsp-ip}

dsp-ip IDM-PROTOCOL ::= {
  BIND-OPERATION  directoryBind
  OPERATIONS
    {chainedRead | chainedCompare | chainedAbandon | chainedList |
      chainedSearch | chainedAddEntry | chainedRemoveEntry | chainedModifyEntry
      | chainedModifyDN}
  ID              id-idm-dsp
}

DISP-IDM-PDUs ::= IDM-PDU{disp-ip}

disp-ip IDM-PROTOCOL ::= {
  BIND-OPERATION  directoryBind
  OPERATIONS      {requestShadowUpdate | updateShadow | coordinateShadowUpdate}
  ID              id-idm-disp
}

DOP-IDM-PDUs ::= IDM-PDU{dop-ip}

dop-ip IDM-PROTOCOL ::= {
  BIND-OPERATION  directoryBind
  OPERATIONS
    {establishOperationalBinding | modifyOperationalBinding |
      terminateOperationalBinding}
  ID              id-idm-dop
}

-- protocol object identifiers
id-idm-dap OBJECT IDENTIFIER ::= {id-idm 0}

id-idm-dsp OBJECT IDENTIFIER ::= {id-idm 1}
```

```
id-idm-disp OBJECT IDENTIFIER ::= {id-idm 2}

id-idm-dop OBJECT IDENTIFIER ::= {id-idm 3}

END -- DirectoryIDMProtocols
```

Annex F

Directory operational binding types

Replace the ASN.1 module in Annex F with the following

```
DirectoryOperationalBindingTypes {joint-iso-itu-t ds(5) module(1)
  directoryOperationalBindingTypes(25) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  id-ob
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6};

id-op-binding-shadow OBJECT IDENTIFIER ::= {id-ob 1}

id-op-binding-hierarchical OBJECT IDENTIFIER ::= {id-ob 2}

id-op-binding-non-specific-hierarchical OBJECT IDENTIFIER ::= {id-ob 3}

END -- DirectoryOperationalBindingTypes
```

ISO/IEC 9594-6 : 2008, Information Technology - Open systems Interconnection - The Directory: Selected attribute types

Working draft for Amendment 1: Communications support enhancements

Add to the end of 2.2:

- IETF RFC3986 (2005), Uniform Resource Identifier (URI): Generic Syntax.
- IETF RFC3406 (2002), Uniform Resource Names (URN) Namespace Definition Mechanisms.
- National Imagery and Mapping Agency (NIMA): TR 8350.2, Word Geodetic System 1984

Add to the end of 2.3:

- ISO/IEC 15961-1:20xx, Information technology – Radio frequency identification (RFID) for item management Data protocol – Part 1: Application interface.
- ISO/IEC 15962:20xx, Information technology – Radio frequency identification – Data protocol: data encoding rules and logical memory functions.

Add to clause 4

URI Uniform Resource Identifier

Add new subsclause:

6.2.12 URI

The *URI* attribute type is used for holding a Uniform Resource Identifier (URI) as defined in RFC 3986.

```
uRI ATTRIBUTE ::= {
  WITH SYNTAX             UTF8String
  EQUALITY MATCHING RULE  caseExactMatch
  ID                      id-at-uRI }
```

Editor's note – Should we rather define the IRI attribute type?

Editor's note – The syntax could instead be

```
WITH SYNTAX UnboundedDirectoryString
      (WITH COMPONENTS {...,teletexString ABSENT})
```

6.2.13 URN

The *URN* attribute type is used for holding a Uniform Resource Name (URN) as defined in RFC 3406.

```
uRN ATTRIBUTE ::= {
  SUBTYPE OF              uRI
  ID                      id-at-uRN }
```

6.2.14 URL

The *URL* attribute type is used for holding a Uniform Resource Name (URL).

```
uRL ATTRIBUTE ::= {
  SUBTYPE OF              uRI
  ID                      id-at-uRL }
```

Add a new subclause 6.3.6:

6.3.6 Coordinates

```
coordinates  ATTRIBUTE  ::=  {
  WITH SYNTAX      Coordinates
  SINGLE VALUE     TRUE
  ID               id-at-coordinates }

Coordinates  ::= SEQUENCE  {
  geodeticDatum     ENUMERATED {
    wsg84   (0) },
  geographicalType  ENUMERATED {
    dms   (0),
    dd    (1),
    dec   (2) },
  latitude          PrintableString,
  longitude         PrintableString }
```

geodeticDatum: This component specifies the type of coordinate system by which the **latitude** and **longitude** components are expressed. It shall take one of the following values:

- **wgs84**: The coordinates are expressed in the World Geodetic System 1984.
- *what else?*

geographicalType: This component gives the syntax of the coordinates given for the **latitude** and **longitude** components. It shall take one of the following values:

– **dms**, which means that the coordinates are given in the degrees-minutes-seconds format. The format shall be ddd:mm:ss optionally followed by a point and a figure indicating tens of seconds. West longitudes and south latitudes are expressed as negative values;

– **dd**, which means that the coordinates are given in degrees and a decimal fraction of a degree; or

NOTE 1 – **dd** 36.5 would be the same value as **dms** 36:30:00.

– **dec**, which means that the coordinates are given as a decimal figure.

NOTE 2 – Notation in **dec** allow s any decimal figure, not necessarily related to degrees (e.g., 2920631).

Change the ASN.1 of 6.12.4 as shown:

```
contentUrl  ATTRIBUTE  ::=  {
  WITH SYNTAX           UnboundDirectoryString
  SUBTYPE Of            uRL
  ID                    id-at-contentUrl }
```

Add three new subsclauses:

6.12.5 UII

The *UII* attribute type is used for holding a Unique Item Identifier (UII).

```
uII ATTRIBUTE ::= {
  WITH SYNTAX             BIT STRING
  EQUALITY MATCHING RULE  bitStringMatch
  ID                      id-at-uII }
```

6.12.6 Tag AFI

The *tag AFI* attribute type is used for holding the AFIs associated with a specific UII structure as defined by a specific object identifier. This object identifier may be held in an attribute of type **tagOid** in the entry in question.

```
tagAfi ATTRIBUTE ::= {
  SYNTAX                  OCTET STRING
  EQUALITY MATCHING RULE  octetStringMatch
  ID                      id-at-tagAfi }
```

6.12.7 Tag location

The *tag location* attribute type is used for holding the position of a tag as expressed in coordinates.

```
tagLocation ATTRIBUTE ::= {
  SUBTYPE OF     coordinates
  SINGLE VALUE   TRUE
  ID             id-at-tagLocation }
```

Annex A

Selected attribute types in ASN.1

Replace the ASN.1 module in Annex A with the following

```
SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
  selectedAttributeTypes(5) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  directoryAbstractService, id-at, id-avc, id-cat, id-mr, id-not, id-pr,
    informationFramework, serviceAdministration
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Attribute{}, ATTRIBUTE, AttributeType, AttributeValueAssertion, CONTEXT,
    ContextAssertion, DistinguishedName, distinguishedNameMatch,
    MAPPING-BASED-MATCHING{}, MATCHING-RULE, OBJECT-CLASS,
    objectIdentifierMatch, SupportedAttributes
    FROM InformationFramework informationFramework
  AttributeCombination, ContextCombination, MRMapping
    FROM ServiceAdministration serviceAdministration
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  FilterItem, HierarchySelections, SearchControlOptions, ServiceControlOptions
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.411 | ISO/IEC 10021-4
  G3FacsimileNonBasicParameters
    FROM MTSAbstractService {joint-iso-itu-t mhs(6) mts(3) modules(0)
      mts-abstract-service(1) version-1999(1)};

/*from IETF RFC 3727

The following import is provided for information only (see 7.2.16), it is not referenced
by any ASN.1 construct within these Directory Specifications. Note that the ASN.1 module
in RFC 3727 imports from the InformationFramework module of edition 4 of ITU-T Rec. X.501
| ISO/IEC 9594-2. A specification importing from both these Directory Specifications and
from RFC 3727 should take corrective actions, e.g., by making a copy of the ASN.1 module
of
RFC 3727 and then update the IMPORT statement.

     allComponentsMatch, componentFilterMatch, directoryComponentsMatch, presentMatch,
rdnMatch
          FROM ComponentMatching {iso(1) 2 36 79672281 xed(3) module (0)
          component-matching(4)} */
-- Directory string type
UnboundedDirectoryString ::= CHOICE {
  teletexString    TeletexString(SIZE (1..MAX)),
  printableString  PrintableString(SIZE (1..MAX)),
  bmpString        BMPString(SIZE (1..MAX)),
  universalString  UniversalString(SIZE (1..MAX)),
  uTF8String       UTF8String(SIZE (1..MAX))
}

DirectoryString{INTEGER:maxSize} ::= CHOICE {
  teletexString    TeletexString(SIZE (1..maxSize,...)),
  printableString  PrintableString(SIZE (1..maxSize,...)),
  bmpString        BMPString(SIZE (1..maxSize,...)),
```

```
  universalString  UniversalString(SIZE (1..maxSize,...)),
  uTF8String       UTF8String(SIZE (1..maxSize,...))
}

-- Attribute types
knowledgeInformation ATTRIBUTE ::= {
  WITH SYNTAX             UnboundedDirectoryString
  EQUALITY MATCHING RULE  caseIgnoreMatch
  ID                      id-at-knowledgeInformation
}

name ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-name
}

commonName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-commonName
}

surname ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-surname
}

givenName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-givenName
}

initials ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-initials
}

generationQualifier ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-generationQualifier
}

uniqueIdentifier ATTRIBUTE ::= {
  WITH SYNTAX             UniqueIdentifier
  EQUALITY MATCHING RULE  bitStringMatch
  ID                      id-at-uniqueIdentifier
}

UniqueIdentifier ::= BIT STRING

dnQualifier ATTRIBUTE ::= {
  WITH SYNTAX               PrintableString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  ORDERING MATCHING RULE    caseIgnoreOrderingMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-dnQualifier
}

serialNumber ATTRIBUTE ::= {
  WITH SYNTAX               PrintableString(SIZE (1..MAX))
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
```

```
  ID                        id-at-serialNumber
}

pseudonym ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-pseudonym
}

uUIDPair ATTRIBUTE ::= {
  WITH SYNTAX             UUIDPair
  EQUALITY MATCHING RULE  uUIDPairMatch
  ID                      id-at-uuidpair
}

UUIDPair ::= SEQUENCE {issuerUUID   UUID,
                       subjectUUID  UUID,
                       ...
}

UUID ::= OCTET STRING(SIZE (16)) -- UUID format only


countryName ATTRIBUTE ::= {
  SUBTYPE OF    name
  WITH SYNTAX   CountryName
  SINGLE VALUE  TRUE
  ID            id-at-countryName
}

CountryName ::= PrintableString(SIZE (2)) -- ISO 3166 codes only


localityName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-localityName
}

collectiveLocalityName ATTRIBUTE ::= {
  SUBTYPE OF  localityName
  COLLECTIVE  TRUE
  ID          id-at-collectiveLocalityName
}

stateOrProvinceName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-stateOrProvinceName
}

collectiveStateOrProvinceName ATTRIBUTE ::= {
  SUBTYPE OF  stateOrProvinceName
  COLLECTIVE  TRUE
  ID          id-at-collectiveStateOrProvinceName
}

streetAddress ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-streetAddress
}

collectiveStreetAddress ATTRIBUTE ::= {
  SUBTYPE OF  streetAddress
  COLLECTIVE  TRUE
  ID          id-at-collectiveStreetAddress
```

```
}

houseIdentifier ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-houseIdentifier
}

organizationName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-organizationName
}

collectiveOrganizationName ATTRIBUTE ::= {
  SUBTYPE OF  organizationName
  COLLECTIVE  TRUE
  ID          id-at-collectiveOrganizationName
}

organizationalUnitName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-organizationalUnitName
}

collectiveOrganizationalUnitName ATTRIBUTE ::= {
  SUBTYPE OF  organizationalUnitName
  COLLECTIVE  TRUE
  ID          id-at-collectiveOrganizationalUnitName
}

title ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-title
}

description ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-description
}

searchGuide ATTRIBUTE ::= {WITH SYNTAX  Guide
                           ID           id-at-searchGuide
}

Guide ::= SET {
  objectClass  [0]  OBJECT-CLASS.&id OPTIONAL,
  criteria     [1]  Criteria,
  ...
}

Criteria ::= CHOICE {
  type  [0]  CriteriaItem,
  and   [1]  SET OF Criteria,
  or    [2]  SET OF Criteria,
  not   [3]  Criteria,
  ...
}

CriteriaItem ::= CHOICE {
  equality          [0]  AttributeType,
  substrings        [1]  AttributeType,
  greaterOrEqual    [2]  AttributeType,
```

```
  lessOrEqual       [3]  AttributeType,
  approximateMatch  [4]  AttributeType,
  ...
}

enhancedSearchGuide ATTRIBUTE ::= {
  WITH SYNTAX  EnhancedGuide
  ID           id-at-enhancedSearchGuide
}

EnhancedGuide ::= SEQUENCE {
  objectClass  [0]  OBJECT-CLASS.&id,
  criteria     [1]  Criteria,
  subset
    [2]  INTEGER {baseObject(0), oneLevel(1), wholeSubtree(2)} DEFAULT oneLevel,
  ...
}

businessCategory ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-businessCategory
}

postalAddress ATTRIBUTE ::= {
  WITH SYNTAX               PostalAddress
  EQUALITY MATCHING RULE    caseIgnoreListMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreListSubstringsMatch
  ID                        id-at-postalAddress
}

PostalAddress ::= SEQUENCE SIZE (1..MAX) OF UnboundedDirectoryString

collectivePostalAddress ATTRIBUTE ::= {
  SUBTYPE OF  postalAddress
  COLLECTIVE  TRUE
  ID          id-at-collectivePostalAddress
}

postalCode ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-postalCode
}

collectivePostalCode ATTRIBUTE ::= {
  SUBTYPE OF  postalCode
  COLLECTIVE  TRUE
  ID          id-at-collectivePostalCode
}

postOfficeBox ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-postOfficeBox
}

collectivePostOfficeBox ATTRIBUTE ::= {
  SUBTYPE OF  postOfficeBox
  COLLECTIVE  TRUE
  ID          id-at-collectivePostOfficeBox
}

physicalDeliveryOfficeName ATTRIBUTE ::= {
  WITH SYNTAX               UnboundedDirectoryString
```

```
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-physicalDeliveryOfficeName
}

collectivePhysicalDeliveryOfficeName ATTRIBUTE ::= {
  SUBTYPE OF  physicalDeliveryOfficeName
  COLLECTIVE  TRUE
  ID          id-at-collectivePhysicalDeliveryOfficeName
}

telephoneNumber ATTRIBUTE ::= {
  WITH SYNTAX               TelephoneNumber
  EQUALITY MATCHING RULE    telephoneNumberMatch
  SUBSTRINGS MATCHING RULE  telephoneNumberSubstringsMatch
  ID                        id-at-telephoneNumber
}

TelephoneNumber ::= PrintableString(SIZE (1..ub-telephone-number))

-- String complying with ITU-T Rec. E.123 only
ub-telephone-number INTEGER ::=
  32

collectiveTelephoneNumber ATTRIBUTE ::= {
  SUBTYPE OF  telephoneNumber
  COLLECTIVE  TRUE
  ID          id-at-collectiveTelephoneNumber
}

telexNumber ATTRIBUTE ::= {
  WITH SYNTAX  TelexNumber
  ID           id-at-telexNumber
}

TelexNumber ::= SEQUENCE {
  telexNumber  PrintableString(SIZE (1..ub-telex-number)),
  countryCode  PrintableString(SIZE (1..ub-country-code)),
  answerback   PrintableString(SIZE (1..ub-answerback)),
  ...
}

ub-telex-number INTEGER ::= 14

ub-country-code INTEGER ::= 4

ub-answerback INTEGER ::= 8

collectiveTelexNumber ATTRIBUTE ::= {
  SUBTYPE OF  telexNumber
  COLLECTIVE  TRUE
  ID          id-at-collectiveTelexNumber
}

facsimileTelephoneNumber ATTRIBUTE ::= {
  WITH SYNTAX               FacsimileTelephoneNumber
  EQUALITY MATCHING RULE    facsimileNumberMatch
  SUBSTRINGS MATCHING RULE  facsimileNumberSubstringsMatch
  ID                        id-at-facsimileTelephoneNumber
}

FacsimileTelephoneNumber ::= SEQUENCE {
  telephoneNumber  TelephoneNumber,
  parameters       G3FacsimileNonBasicParameters OPTIONAL,
  ...
}

collectiveFacsimileTelephoneNumber ATTRIBUTE ::= {
```

```
  SUBTYPE OF  facsimileTelephoneNumber
  COLLECTIVE  TRUE
  ID          id-at-collectiveFacsimileTelephoneNumber
}

x121Address ATTRIBUTE ::= {
  WITH SYNTAX               X121Address
  EQUALITY MATCHING RULE    numericStringMatch
  SUBSTRINGS MATCHING RULE  numericStringSubstringsMatch
  ID                        id-at-x121Address
}

X121Address ::= NumericString(SIZE (1..ub-x121-address))

-- String as defined by ITU-T Rec. X.121
ub-x121-address INTEGER ::= 15

internationalISDNNumber ATTRIBUTE ::= {
  WITH SYNTAX               InternationalISDNNumber
  EQUALITY MATCHING RULE    numericStringMatch
  SUBSTRINGS MATCHING RULE  numericStringSubstringsMatch
  ID                        id-at-internationalISDNNumber
}

InternationalISDNNumber ::=
  NumericString(SIZE (1..ub-international-isdn-number))

-- String complying with ITU-T Rec. E.164 only
ub-international-isdn-number INTEGER ::=
  16

collectiveInternationalISDNNumber ATTRIBUTE ::= {
  SUBTYPE OF  internationalISDNNumber
  COLLECTIVE  TRUE
  ID          id-at-collectiveInternationalISDNNumber
}

registeredAddress ATTRIBUTE ::= {
  SUBTYPE OF   postalAddress
  WITH SYNTAX  PostalAddress
  ID           id-at-registeredAddress
}

destinationIndicator ATTRIBUTE ::= {
  WITH SYNTAX               DestinationIndicator
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-destinationIndicator
}

DestinationIndicator ::= PrintableString(SIZE (1..MAX))

-- alphabetical characters only
communicationsService ATTRIBUTE ::= {
  WITH SYNTAX             CommunicationsService
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-at-communicationsService
}

CommunicationsService ::= OBJECT IDENTIFIER

communicationsNetwork ATTRIBUTE ::= {
  WITH SYNTAX             CommunicationsNetwork
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  ID                      id-at-communicationsNetwork
}
```

```
CommunicationsNetwork ::= OBJECT IDENTIFIER

preferredDeliveryMethod ATTRIBUTE ::= {
  WITH SYNTAX   PreferredDeliveryMethod
  SINGLE VALUE  TRUE
  ID            id-at-preferredDeliveryMethod
}

PreferredDeliveryMethod ::=
  SEQUENCE OF
    INTEGER {any-delivery-method(0), mhs-delivery(1), physical-delivery(2),
             telex-delivery(3), teletex-delivery(4), g3-facsimile-delivery(5),
             g4-facsimile-delivery(6), ia5-terminal-delivery(7),
             videotex-delivery(8), telephone-delivery(9)}

presentationAddress ATTRIBUTE ::= {
  WITH SYNTAX             PresentationAddress
  EQUALITY MATCHING RULE  presentationAddressMatch
  SINGLE VALUE            TRUE
  ID                      id-at-presentationAddress
}

PresentationAddress ::= SEQUENCE {
  pSelector   [0]  OCTET STRING OPTIONAL,
  sSelector   [1]  OCTET STRING OPTIONAL,
  tSelector   [2]  OCTET STRING OPTIONAL,
  nAddresses  [3]  SET SIZE (1..MAX) OF OCTET STRING,
  ...
}

supportedApplicationContext ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-at-supportedApplicationContext
}

protocolInformation ATTRIBUTE ::= {
  WITH SYNTAX             ProtocolInformation
  EQUALITY MATCHING RULE  protocolInformationMatch
  ID                      id-at-protocolInformation
}

ProtocolInformation ::= SEQUENCE {
  nAddress  OCTET STRING,
  profiles  SET OF OBJECT IDENTIFIER
}

distinguishedName ATTRIBUTE ::= {
  WITH SYNTAX             DistinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  ID                      id-at-distinguishedName
}

member ATTRIBUTE ::= {SUBTYPE OF  distinguishedName
                      ID          id-at-member
}

uniqueMember ATTRIBUTE ::= {
  WITH SYNTAX             NameAndOptionalUID
  EQUALITY MATCHING RULE  uniqueMemberMatch
  ID                      id-at-uniqueMember
}

NameAndOptionalUID ::= SEQUENCE {
  dn   DistinguishedName,
  uid  UniqueIdentifier OPTIONAL,
  ...
}
```

```
owner ATTRIBUTE ::= {SUBTYPE OF  distinguishedName
                     ID          id-at-owner
}

roleOccupant ATTRIBUTE ::= {
  SUBTYPE OF  distinguishedName
  ID          id-at-roleOccupant
}

seeAlso ATTRIBUTE ::= {SUBTYPE OF  distinguishedName
                       ID          id-at-seeAlso
}

dmdName ATTRIBUTE ::= {
  SUBTYPE OF   name
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-dmdName
}

--  Attributes for tag-based identification
tagOid ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  ID                      id-at-tagOid
}

uiiFormat ATTRIBUTE ::= {
  WITH SYNTAX   UnboundedDirectoryString
  SINGLE VALUE  TRUE
  ID            id-at-uiiFormat
}

uiiInUrn ATTRIBUTE ::= {
  WITH SYNTAX             UTF8String
  EQUALITY MATCHING RULE  caseExactMatch
  SINGLE VALUE            TRUE
  ID                      id-at-uiiInUrn
}

contentUri ATTRIBUTE ::= {
  WITH SYNTAX  UnboundedDirectoryString
  ID           id-at-contentUri
}

-- Notification attributes
dSAProblem ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-not-dSAProblem
}

searchServiceProblem ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  ID                      id-not-searchServiceProblem
}

serviceType ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  SINGLE VALUE            TRUE
  ID                      id-not-serviceType
}

attributeTypeList ATTRIBUTE ::= {
```

```
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-not-attributeTypeList
}

matchingRuleList ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-not-matchingRuleList
}

filterItem ATTRIBUTE ::= {
  WITH SYNTAX  FilterItem
  ID           id-not-filterItem
}

attributeCombinations ATTRIBUTE ::= {
  WITH SYNTAX  AttributeCombination
  ID           id-not-attributeCombinations
}

contextTypeList ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-not-contextTypeList
}

contextList ATTRIBUTE ::= {
  WITH SYNTAX  ContextAssertion
  ID           id-not-contextList
}

contextCombinations ATTRIBUTE ::= {
  WITH SYNTAX  ContextCombination
  ID           id-not-contextCombinations
}

hierarchySelectList ATTRIBUTE ::= {
  WITH SYNTAX   HierarchySelections
  SINGLE VALUE  TRUE
  ID            id-not-hierarchySelectList
}

searchControlOptionsList ATTRIBUTE ::= {
  WITH SYNTAX   SearchControlOptions
  SINGLE VALUE  TRUE
  ID            id-not-searchControlOptionsList
}

serviceControlOptionsList ATTRIBUTE ::= {
  WITH SYNTAX   ServiceControlOptions
  SINGLE VALUE  TRUE
  ID            id-not-serviceControlOptionsList
}

multipleMatchingLocalities ATTRIBUTE ::= {
  WITH SYNTAX  MultipleMatchingLocalities
  ID           id-not-multipleMatchingLocalities
}

MultipleMatchingLocalities ::= SEQUENCE {
  matchingRuleUsed  MATCHING-RULE.&id OPTIONAL,
  attributeList     SEQUENCE OF AttributeValueAssertion,
  ...
}

proposedRelaxation ATTRIBUTE ::= {
  WITH SYNTAX  MRMappings
```

```
  ID           id-not-proposedRelaxation
}

MRMappings ::= SEQUENCE OF MRMapping

appliedRelaxation ATTRIBUTE ::= {
  WITH SYNTAX             OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                      id-not-appliedRelaxation
}

-- Matching rules
caseExactMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-caseExactMatch
}

caseIgnoreMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-caseIgnoreMatch
}

caseExactOrderingMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-caseExactOrderingMatch
}

caseIgnoreOrderingMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-caseIgnoreOrderingMatch
}

caseExactSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion -- only the PrintableString choice
  ID      id-mr-caseExactSubstringsMatch
}

caseIgnoreSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-caseIgnoreSubstringsMatch
}

SubstringAssertion ::=
  SEQUENCE OF
    CHOICE {initial  [0]  UnboundedDirectoryString,
            any      [1]  UnboundedDirectoryString,
            final    [2]  UnboundedDirectoryString,
            control  Attribute{{SupportedAttributes}},
            ...
    } --  Used to specify interpretation of the following items

-- at most one initial and one final component
numericStringMatch MATCHING-RULE ::= {
  SYNTAX  NumericString
  ID      id-mr-numericStringMatch
}

numericStringOrderingMatch MATCHING-RULE ::= {
  SYNTAX  NumericString
  ID      id-mr-numericStringOrderingMatch
}

numericStringSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-numericStringSubstringsMatch
}

caseIgnoreListMatch MATCHING-RULE ::= {
```

```
  SYNTAX  CaseIgnoreList
  ID      id-mr-caseIgnoreListMatch
}

CaseIgnoreList ::= SEQUENCE OF UnboundedDirectoryString

caseIgnoreListSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-caseIgnoreListSubstringsMatch
}

storedPrefixMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-storedPrefixMatch
}

booleanMatch MATCHING-RULE ::= {SYNTAX  BOOLEAN
                                ID      id-mr-booleanMatch
}

integerMatch MATCHING-RULE ::= {SYNTAX  INTEGER
                                ID      id-mr-integerMatch
}

integerOrderingMatch MATCHING-RULE ::= {
  SYNTAX  INTEGER
  ID      id-mr-integerOrderingMatch
}

bitStringMatch MATCHING-RULE ::= {
  SYNTAX  BIT STRING
  ID      id-mr-bitStringMatch
}

octetStringMatch MATCHING-RULE ::= {
  SYNTAX  OCTET STRING
  ID      id-mr-octetStringMatch
}

octetStringOrderingMatch MATCHING-RULE ::= {
  SYNTAX  OCTET STRING
  ID      id-mr-octetStringOrderingMatch
}

octetStringSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  OctetSubstringAssertion
  ID      id-mr-octetStringSubstringsMatch
}

OctetSubstringAssertion ::=
  SEQUENCE OF
    CHOICE {initial  [0]  OCTET STRING,
            any      [1]  OCTET STRING,
            final    [2]  OCTET STRING,
            ...}

-- at most one initial and one final component
telephoneNumberMatch MATCHING-RULE ::= {
  SYNTAX  TelephoneNumber
  ID      id-mr-telephoneNumberMatch
}

telephoneNumberSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-telephoneNumberSubstringsMatch
}

presentationAddressMatch MATCHING-RULE ::= {
```

```
  SYNTAX  PresentationAddress
  ID      id-mr-presentationAddressMatch
}

uniqueMemberMatch MATCHING-RULE ::= {
  SYNTAX  NameAndOptionalUID
  ID      id-mr-uniqueMemberMatch
}

protocolInformationMatch MATCHING-RULE ::= {
  SYNTAX  OCTET STRING
  ID      id-mr-protocolInformationMatch
}

facsimileNumberMatch MATCHING-RULE ::= {
  SYNTAX  TelephoneNumber
  ID      id-mr-facsimileNumberMatch
}

facsimileNumberSubstringsMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-facsimileNumberSubstringsMatch
}

uUIDPairMatch MATCHING-RULE ::= {SYNTAX  UUIDPair
                                 ID      id-mr-uuidpairmatch
}

uTCTimeMatch MATCHING-RULE ::= {SYNTAX  UTCTime
                                ID      id-mr-uTCTimeMatch
}

uTCTimeOrderingMatch MATCHING-RULE ::= {
  SYNTAX  UTCTime
  ID      id-mr-uTCTimeOrderingMatch
}

generalizedTimeMatch MATCHING-RULE ::= {
  SYNTAX  GeneralizedTime
  -- as per 46.3 b) or c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
  ID      id-mr-generalizedTimeMatch
}

generalizedTimeOrderingMatch MATCHING-RULE ::= {
  SYNTAX  GeneralizedTime
  -- as per 46.3 b) or c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
  ID      id-mr-generalizedTimeOrderingMatch
}

systemProposedMatch MATCHING-RULE ::= {ID  id-mr-systemProposedMatch
}

integerFirstComponentMatch MATCHING-RULE ::= {
  SYNTAX  INTEGER
  ID      id-mr-integerFirstComponentMatch
}

objectIdentifierFirstComponentMatch MATCHING-RULE ::= {
  SYNTAX  OBJECT IDENTIFIER
  ID      id-mr-objectIdentifierFirstComponentMatch
}

directoryStringFirstComponentMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-directoryStringFirstComponentMatch
}

wordMatch MATCHING-RULE ::= {
```

```
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-wordMatch
}

keywordMatch MATCHING-RULE ::= {
  SYNTAX  UnboundedDirectoryString
  ID      id-mr-keywordMatch
}

generalWordMatch MATCHING-RULE ::= {
  SYNTAX  SubstringAssertion
  ID      id-mr-generalWordMatch
}

sequenceMatchType ATTRIBUTE ::= {
  WITH SYNTAX   SequenceMatchType
  SINGLE VALUE  TRUE
  ID            id-cat-sequenceMatchType
} -- defaulting to sequenceExact

SequenceMatchType ::= ENUMERATED {
  sequenceExact(0), sequenceDeletion(1), sequenceRestrictedDeletion(2),
  sequencePermutation(3), sequencePermutationAndDeletion(4),
  sequenceProviderDefined(5),...}

wordMatchTypes ATTRIBUTE ::= {
  WITH SYNTAX   WordMatchTypes
  SINGLE VALUE  TRUE
  ID            id-cat-wordMatchType
} -- defaulting to wordExact

WordMatchTypes ::= ENUMERATED {
  wordExact(0), wordTruncated(1), wordPhonetic(2), wordProviderDefined(3),...
}

characterMatchTypes ATTRIBUTE ::= {
  WITH SYNTAX   CharacterMatchTypes
  SINGLE VALUE  TRUE
  ID            id-cat-characterMatchTypes
}

CharacterMatchTypes ::= ENUMERATED {
  characterExact(0), characterCaseIgnore(1), characterMapped(2),...}

selectedContexts ATTRIBUTE ::= {
  WITH SYNTAX  ContextAssertion
  ID           id-cat-selectedContexts
}

approximateStringMatch MATCHING-RULE ::= {ID  id-mr-approximateStringMatch
}

ignoreIfAbsentMatch MATCHING-RULE ::= {ID  id-mr-ignoreIfAbsentMatch
}

nullMatch MATCHING-RULE ::= {ID  id-mr-nullMatch
}

ZONAL-MATCHING ::=
  MAPPING-BASED-MATCHING{ZonalSelect, TRUE, ZonalResult, zonalMatch.&id}

ZonalSelect ::= SEQUENCE OF AttributeType

ZonalResult ::= ENUMERATED {
  cannot-select-mapping(0), zero-mappings(2), multiple-mappings(3),...}

zonalMatch MATCHING-RULE ::= {
  UNIQUE-MATCH-INDICATOR  multipleMatchingLocalities
```

```
  ID                      id-mr-zonalMatch
}

-- Contexts
languageContext CONTEXT ::= {
  WITH SYNTAX  LanguageContextSyntax
  ID           id-avc-language
}

LanguageContextSyntax ::= PrintableString(SIZE (2..3)) -- ISO 639-2 codes only


temporalContext CONTEXT ::= {
  WITH SYNTAX  TimeSpecification
  ASSERTED AS  TimeAssertion
  ID           id-avc-temporal
}

TimeSpecification ::= SEQUENCE {
  time
    CHOICE {absolute
              SEQUENCE {startTime  [0]  GeneralizedTime OPTIONAL,
                        endTime    [1]  GeneralizedTime OPTIONAL,
                        ...},
            periodic  SET SIZE (1..MAX) OF Period},
  notThisTime  BOOLEAN DEFAULT FALSE,
  timeZone     TimeZone OPTIONAL,
  ...
}

Period ::= SEQUENCE {
  timesOfDay  [0]  SET SIZE (1..MAX) OF DayTimeBand OPTIONAL,
  days
    [1]  CHOICE {intDay  SET OF INTEGER,
                 bitDay
                   BIT STRING {sunday(0), monday(1), tuesday(2), wednesday(3),
                               thursday(4), friday(5), saturday(6)},
                 dayOf   XDayOf,
                 ...} OPTIONAL,
  weeks
    [2]  CHOICE {allWeeks  NULL,
                 intWeek   SET OF INTEGER,
                 bitWeek
                   BIT STRING {week1(0), week2(1), week3(2), week4(3), week5(4)},
                 ...
  } OPTIONAL,
  months
    [3]  CHOICE {allMonths  NULL,
                 intMonth   SET OF INTEGER,
                 bitMonth
                   BIT STRING {january(0), february(1), march(2), april(3),
                               may(4), june(5), july(6), august(7),
                               september(8), october(9), november(10),
                               december(11)},
                 ...} OPTIONAL,
  years       [4]  SET OF INTEGER(1000..MAX) OPTIONAL,
  ...
}

XDayOf ::= CHOICE {
  first   [1]  NamedDay,
  second  [2]  NamedDay,
  third   [3]  NamedDay,
  fourth  [4]  NamedDay,
  fifth   [5]  NamedDay
}

NamedDay ::= CHOICE {
```

```
  intNamedDays
    ENUMERATED {sunday(1), monday(2), tuesday(3), wednesday(4), thursday(5),
                friday(6), saturday(7)},
  bitNamedDays
    BIT STRING {sunday(0), monday(1), tuesday(2), wednesday(3), thursday(4),
                friday(5), saturday(6)}
}

DayTimeBand ::= SEQUENCE {
  startDayTime  [0]  DayTime DEFAULT {hour 0},
  endDayTime    [1]  DayTime DEFAULT {hour 23, minute 59, second 59},
  ...
}

DayTime ::= SEQUENCE {
  hour    [0]  INTEGER(0..23),
  minute  [1]  INTEGER(0..59) DEFAULT 0,
  second  [2]  INTEGER(0..59) DEFAULT 0,
  ...
}

TimeZone ::= INTEGER(-12..12)

TimeAssertion ::= CHOICE {
  now      NULL,
  at       GeneralizedTime,
  between
    SEQUENCE {startTime  [0]  GeneralizedTime,
              endTime    [1]  GeneralizedTime OPTIONAL,
              entirely   BOOLEAN DEFAULT FALSE,
              ...},
  ...
}

localeContext CONTEXT ::= {
  WITH SYNTAX  LocaleContextSyntax
  ID           id-avc-locale
}

LocaleContextSyntax ::= CHOICE {
  localeID1  OBJECT IDENTIFIER,
  localeID2  UnboundedDirectoryString,
  ...
}

ldapAttributeOptionContext CONTEXT ::= {
  WITH SYNTAX   AttributeOptionList
  ASSERTED AS   AttributeOptionList
  ABSENT-MATCH  FALSE
  ID            id-avc-ldapAttributeOption
}

AttributeOptionList ::= SEQUENCE OF UTF8String

-- Object identifier assignments
-- object identifiers assigned in other modules are shown in comments
-- Attributes
-- id-at-objectClass                              OBJECT IDENTIFIER  ::=  {id-at 0}
-- id-at-aliasedEntryName                      OBJECT IDENTIFIER  ::=  {id-at 1}
-- id-at-encryptedAliasedEntryName                OBJECT IDENTIFIER  ::=  {id-at 1 2}
id-at-knowledgeInformation OBJECT IDENTIFIER ::=
  {id-at 2}

id-at-commonName OBJECT IDENTIFIER ::= {id-at 3}

-- id-at-encryptedCommonName                   OBJECT IDENTIFIER  ::=  {id-at 3 2}
id-at-surname OBJECT IDENTIFIER ::=
  {id-at 4}
```

```
-- id-at-encryptedSurname                       OBJECT IDENTIFIER  ::=  {id-at 4 2}
id-at-serialNumber OBJECT IDENTIFIER ::=
  {id-at 5}

-- id-at-encryptedSerialNumbe   r               OBJECT IDENTIFIER  ::=  {id-at 5 2}
id-at-countryName OBJECT IDENTIFIER ::=
  {id-at 6}

-- id-at-encryptedCountryName                   OBJECT IDENTIFIER  ::=  {id-at 6 2}
id-at-localityName OBJECT IDENTIFIER ::=
  {id-at 7}

-- id-at-encryptedLocalityName                      OBJECT IDENTIFIER  ::=  {id-at 7 2}
id-at-collectiveLocalityName OBJECT IDENTIFIER ::=
  {id-at 7 1}

-- id-at-encryptedCollectiveLocalityName            OBJECT IDENTIFIER  ::=  {id-at 7 1 2}
id-at-stateOrProvinceName OBJECT IDENTIFIER ::=
  {id-at 8}

-- id-at-encryptedStateOrProvinceName           OBJECT IDENTIFIER  ::=  {id-at 8 2}
id-at-collectiveStateOrProvinceName OBJECT IDENTIFIER ::=
  {id-at 8 1}

-- id-at-encryptedCollectiveStateOrProvinceName     OBJECT IDENTIFIER  ::=  {id-at 8 1 2}
id-at-streetAddress OBJECT IDENTIFIER ::=
  {id-at 9}

-- id-at-encryptedStreetAddress                     OBJECT IDENTIFIER  ::=  {id-at 9 2}
id-at-collectiveStreetAddress OBJECT IDENTIFIER ::=
  {id-at 9 1}

-- id-at-encryptedCollectiveStreetAddress           OBJECT IDENTIFIER  ::=  {id-at 9 1 2}
id-at-organizationName OBJECT IDENTIFIER ::=
  {id-at 10}

-- id-at-encryptedOrganizationName                  OBJECT IDENTIFIER  ::=  {id-at 10 2}
id-at-collectiveOrganizationName OBJECT IDENTIFIER ::=
  {id-at 10 1}

-- id-at-encryptedCollectiveOrganizationName        OBJECT IDENTIFIER  ::=  {id-at 10 1
2}
id-at-organizationalUnitName OBJECT IDENTIFIER ::=
  {id-at 11}

-- id-at-encryptedOrganizationalUnitName            OBJECT IDENTIFIER  ::=  {id-at 11 2}
id-at-collectiveOrganizationalUnitName OBJECT IDENTIFIER ::=
  {id-at 11 1}

-- id-at-encryptedCollectiveOrganizationalUnitNam       OBJECT IDENTIFIER  ::=  {id-at
11 1 2}
id-at-title OBJECT IDENTIFIER ::=
  {id-at 12}

-- id-at-encryptedTitle                         OBJECT IDENTIFIER  ::=  {id-at 12 2}
id-at-description OBJECT IDENTIFIER ::=
  {id-at 13}

-- id-at-encryptedDescription                       OBJECT IDENTIFIER  ::=  {id-at 13 2}
id-at-searchGuide OBJECT IDENTIFIER ::=
  {id-at 14}

-- id-at-encryptedSearchGuide                       OBJECT IDENTIFIER  ::=  {id-at 14 2}
id-at-businessCategory OBJECT IDENTIFIER ::=
  {id-at 15}

-- id-at-encryptedBusinessCategory                  OBJECT IDENTIFIER  ::=  {id-at 15 2}
```

```
id-at-postalAddress OBJECT IDENTIFIER ::=
  {id-at 16}

-- id-at-encryptedPostalAddress                    OBJECT IDENTIFIER  ::=  {id-at 16 2}
id-at-collectivePostalAddress OBJECT IDENTIFIER ::=
  {id-at 16 1}

-- id-at-encryptedCollectivePostalAddress          OBJECT IDENTIFIER  ::=  {id-at 16 1
2}
id-at-postalCode OBJECT IDENTIFIER ::=
  {id-at 17}

-- id-at-encryptedPostalCode                  OBJECT IDENTIFIER  ::=  {id-at 17 2}
id-at-collectivePostalCode OBJECT IDENTIFIER ::=
  {id-at 17 1}

-- id-at-encryptedCollectivePostalCode             OBJECT IDENTIFIER  ::=  {id-at 17 1
2}
id-at-postOfficeBox OBJECT IDENTIFIER ::=
  {id-at 18}

id-at-collectivePostOfficeBox OBJECT IDENTIFIER ::= {id-at 18 1}

-- id-at-encryptedPostOfficeBox                    OBJECT IDENTIFIER  ::=  {id-at 18 2}
-- id-at-encryptedCollectivePostOfficeBox          OBJECT IDENTIFIER  ::=  {id-at 18 1
2}
id-at-physicalDeliveryOfficeName OBJECT IDENTIFIER ::=
  {id-at 19}

id-at-collectivePhysicalDeliveryOfficeName OBJECT IDENTIFIER ::= {id-at 19 1}

-- id-at-encryptedPhysicalDeliveryOfficeName       OBJECT IDENTIFIER  ::=  {id-at 19 2}
-- id-at-encryptedCollectivePhysicalDeliveryOfficeName   OBJECT IDENTIFIER  ::=  {id-at
19 1 2}
id-at-telephoneNumber OBJECT IDENTIFIER ::=
  {id-at 20}

-- id-at-encryptedTelephoneNumber             OBJECT IDENTIFIER  ::=  {id-at 20 2}
id-at-collectiveTelephoneNumber OBJECT IDENTIFIER ::=
  {id-at 20 1}

-- id-at-encryptedCollectiveTelephoneNumber        OBJECT IDENTIFIER  ::=  {id-at 20 1
2}
id-at-telexNumber OBJECT IDENTIFIER ::=
  {id-at 21}

-- id-at-encryptedTelexNumber                      OBJECT IDENTIFIER  ::=  {id-at 21 2}
id-at-collectiveTelexNumber OBJECT IDENTIFIER ::=
  {id-at 21 1}

-- id-at-encryptedCollectiveTelexNumber            OBJECT IDENTIFIER  ::=  {id-at 21 1
2}
-- id-at-teletexTerminalIdentifier                 OBJECT IDENTIFIER  ::=  {id-at 22}
-- id-at-encryptedTeletexTerminalIdentifier             OBJECT IDENTIFIER  ::=  {id-at
22 2}
-- id-at-collectiveTeletexTerminalIdentifier            OBJECT IDENTIFIER  ::=  {id-at
22 1}
-- id-at-encryptedCollectiveTeletexTerminalIdentifier   OBJECT IDENTIFIER  ::=  {id-at
22 1 2}
id-at-facsimileTelephoneNumber OBJECT IDENTIFIER ::=
  {id-at 23}

-- id-at-encryptedFacsimileTelephoneNumber     OBJECT IDENTIFIER  ::=  {id-at 23 2}
id-at-collectiveFacsimileTelephoneNumber OBJECT IDENTIFIER ::=
  {id-at 23 1}

-- id-at-encryptedCollectiveFacsimileTelephoneNumber    OBJECT IDENTIFIER  ::=  {id-at
23 1 2}
```

```
id-at-x121Address OBJECT IDENTIFIER ::=
  {id-at 24}

-- id-at-encryptedX121Address                  OBJECT IDENTIFIER  ::=  {id-at 24 2}
id-at-internationalISDNNumber OBJECT IDENTIFIER ::=
  {id-at 25}

-- id-at-encryptedInternationalISDNNumber           OBJECT IDENTIFIER  ::=  {id-at 25 2}
id-at-collectiveInternationalISDNNumber OBJECT IDENTIFIER ::=
  {id-at 25 1}

-- id-at-encryptedCollectiveInternationalISDNNumber OBJECT IDENTIFIER  ::=  {id-at 25 1
2}
id-at-registeredAddress OBJECT IDENTIFIER ::=
  {id-at 26}

-- id-at-encryptedRegisteredAddress                 OBJECT IDENTIFIER  ::=  {id-at 26 2}
id-at-destinationIndicator OBJECT IDENTIFIER ::=
  {id-at 27}

-- id-at-encryptedDestinationIndicator              OBJECT IDENTIFIER  ::=  {id-at 27 2}
id-at-preferredDeliveryMethod OBJECT IDENTIFIER ::=
  {id-at 28}

-- id-at-encryptedPreferredDeliveryMethod           OBJECT IDENTIFIER  ::=  {id-at 28 2}
id-at-presentationAddress OBJECT IDENTIFIER ::=
  {id-at 29}

-- id-at-encryptedPresentationAddress               OBJECT IDENTIFIER  ::=  {id-at 29 2}
id-at-supportedApplicationContext OBJECT IDENTIFIER ::=
  {id-at 30}

-- id-at-encryptedSupportedApplicationContext       OBJECT IDENTIFIER  ::=  {id-at 30 2}
id-at-member OBJECT IDENTIFIER ::=
  {id-at 31}

-- id-at-encryptedMember                            OBJECT IDENTIFIER  ::=  {id-at 31 2}
id-at-owner OBJECT IDENTIFIER ::=
  {id-at 32}

-- id-at-encryptedOwner                        OBJECT IDENTIFIER  ::=  {id-at 32 2}
id-at-roleOccupant OBJECT IDENTIFIER ::=
  {id-at 33}

-- id-at-encryptedRoleOccupant                 OBJECT IDENTIFIER  ::=  {id-at 33 2}
id-at-seeAlso OBJECT IDENTIFIER ::=
  {id-at 34}

-- id-at-encryptedSeeAlso                           OBJECT IDENTIFIER  ::=  {id-at 34 2}
-- id-at-userPassword                          OBJECT IDENTIFIER  ::=  {id-at 35}
     X.509|Part8
-- id-at-encryptedUserPassword                      OBJECT IDENTIFIER  ::=  {id-at 35 2}
-- id-at-userCertificate                            OBJECT IDENTIFIER  ::=  {id-at 36}
     X.509|Part8
-- id-at-encryptedUserCertificate              OBJECT IDENTIFIER  ::=  {id-at 36 2}
-- id-at-cACertificate                         OBJECT IDENTIFIER  ::=  {id-at 37}
     X.509|Part8
-- id-at-encryptedCACertificate                     OBJECT IDENTIFIER  ::=  {id-at 37 2}
-- id-at-authorityRevocationList                    OBJECT IDENTIFIER  ::=  {id-at 38}
     X.509|Part8
-- id-at-encryptedAuthorityRevocationList           OBJECT IDENTIFIER  ::=  {id-at 38 2}
-- id-at-certificateRevocationList                  OBJECT IDENTIFIER  ::=  {id-at 39}
     X.509|Part8
-- id-at-encryptedCertificateRevocationList             OBJECT IDENTIFIER  ::=  {id-at
39 2}
-- id-at-crossCertificatePair                       OBJECT IDENTIFIER  ::=  {id-at 40}
     X.509|Part8
-- id-at-encryptedCrossCertificatePair              OBJECT IDENTIFIER  ::=  {id-at 40 2}
```

```
id-at-name OBJECT IDENTIFIER ::=
  {id-at 41}

id-at-givenName OBJECT IDENTIFIER ::= {id-at 42}

-- id-at-encryptedGivenName                    OBJECT IDENTIFIER  ::=  {id-at 42 2}
id-at-initials OBJECT IDENTIFIER ::=
  {id-at 43}

-- id-at-encryptedInitials                         OBJECT IDENTIFIER  ::=  {id-at 43 2}
id-at-generationQualifier OBJECT IDENTIFIER ::=
  {id-at 44}

-- id-at-encryptedGenerationQualifier              OBJECT IDENTIFIER  ::=  {id-at 44 2}
id-at-uniqueIdentifier OBJECT IDENTIFIER ::=
  {id-at 45}

-- id-at-encryptedUniqueIdentifier                 OBJECT IDENTIFIER  ::=  {id-at 45 2}
id-at-dnQualifier OBJECT IDENTIFIER ::=
  {id-at 46}

-- id-at-encryptedDnQualifier                      OBJECT IDENTIFIER  ::=  {id-at 46 2}
id-at-enhancedSearchGuide OBJECT IDENTIFIER ::=
  {id-at 47}

-- id-at-encryptedEnhancedSearchGuide          OBJECT IDENTIFIER  ::=  {id-at 47 2}
id-at-protocolInformation OBJECT IDENTIFIER ::=
  {id-at 48}

-- id-at-encryptedProtocolInformation              OBJECT IDENTIFIER  ::=  {id-at 48 2}
id-at-distinguishedName OBJECT IDENTIFIER ::=
  {id-at 49}

-- id-at-encryptedDistinguishedName                OBJECT IDENTIFIER  ::=  {id-at 49 2}
id-at-uniqueMember OBJECT IDENTIFIER ::=
  {id-at 50}

-- id-at-encryptedUniqueMember                 OBJECT IDENTIFIER  ::=  {id-at 50 2}
id-at-houseIdentifier OBJECT IDENTIFIER ::=
  {id-at 51}

-- id-at-encryptedHouseIdentifier              OBJECT IDENTIFIER  ::=  {id-at 51 2}
-- id-at-supportedAlgorithms                   OBJECT IDENTIFIER  ::=  {id-at 52}
     X.509|Part8
-- id-at-encryptedSupportedAlgorithms              OBJECT IDENTIFIER  ::=  {id-at 52 2}
-- id-at-deltaRevocationList                   OBJECT IDENTIFIER  ::=  {id-at 53}
     X.509|Part8
-- id-at-encryptedDeltaRevocationList              OBJECT IDENTIFIER  ::=  {id-at 53 2}
id-at-dmdName OBJECT IDENTIFIER ::=
  {id-at 54}

-- id-at-encryptedDmdName                      OBJECT IDENTIFIER  ::=  {id-at 54 2}
-- id-at-clearance                             OBJECT IDENTIFIER  ::=  {id-at 55}
-- id-at-encryptedClearance                    OBJECT IDENTIFIER  ::=  {id-at 55 2}
-- id-at-defaultDirQop                         OBJECT IDENTIFIER  ::=  {id-at 56}
-- id-at-encryptedDefaultDirQop                    OBJECT IDENTIFIER  ::=  {id-at 56 2}
-- id-at-attributeIntegrityInfo                    OBJECT IDENTIFIER  ::=  {id-at 57}
-- id-at-encryptedAttributeIntegrityInfo               OBJECT IDENTIFIER  ::=  {id-at
57 2}
-- id-at-attributeCertificate                      OBJECT IDENTIFIER  ::=  {id-at
58}  X.509|Part8
-- id-at-encryptedAttributeCertificate             OBJECT IDENTIFIER  ::=  {id-at
58 2}
-- id-at-attributeCertificateRevocationList        OBJECT IDENTIFIER  ::=  {id-at
59}  X.509|Part8
-- id-at-encryptedAttributeCertificateRevocationList   OBJECT IDENTIFIER  ::=  {id-at
59 2}
-- id-at-confKeyInfo                           OBJECT IDENTIFIER  ::=  {id-at 60}
```

```
-- id-at-encryptedConfKeyInfo                    OBJECT IDENTIFIER  ::=  {id-at 60 2}
-- id-at-aACertificate                          OBJECT IDENTIFIER  ::=  {id-at 61}
     X.509|Part8
-- id-at-attributeDescriptorCertificate                OBJECT IDENTIFIER  ::=  {id-at
62}  X.509|Part8
-- id-at-attributeAuthorityRevocationList          OBJECT IDENTIFIER  ::=  {id-at 63}
     X.509|Part8
-- id-at-family-information                       OBJECT IDENTIFIER  ::=  {id-at 64}
id-at-pseudonym OBJECT IDENTIFIER ::=
  {id-at 65}

id-at-communicationsService OBJECT IDENTIFIER ::= {id-at 66}

id-at-communicationsNetwork OBJECT IDENTIFIER ::= {id-at 67}

-- id-at-certificationPracticeStmt                OBJECT IDENTIFIER  ::=  {id-at 68}
     X.509|Part8
-- id-at-certificatePolicy                        OBJECT IDENTIFIER  ::=  {id-at 69}
     X.509|Part8
-- id-at-pkiPath                                OBJECT IDENTIFIER  ::=  {id-at 70}
     X.509|Part8
-- id-at-privPolicy                               OBJECT IDENTIFIER  ::=  {id-at 71}
     X.509|Part8
-- id-at-role                                   OBJECT IDENTIFIER  ::=  {id-at 72}
     X.509|Part8
-- id-at-delegationPath                         OBJECT IDENTIFIER  ::=  {id-at 73}
     X.509|Part8
-- id-at-protPrivPolicy                         OBJECT IDENTIFIER  ::=  {id-at 74}
     X.509|Part8
-- id-at-xMLPrivilegeInfo                         OBJECT IDENTIFIER  ::=  {id-at 75}
     X.509|Part8
-- id-at-xmlPrivPolicy                          OBJECT IDENTIFIER  ::=  {id-at 76}
     X.509|Part8
id-at-uuidpair OBJECT IDENTIFIER ::=
  {id-at 77}

id-at-tagOid OBJECT IDENTIFIER ::= {id-at 78}

id-at-uiiFormat OBJECT IDENTIFIER ::= {id-at 79}

id-at-uiiInUrn OBJECT IDENTIFIER ::= {id-at 80}

id-at-contentUri OBJECT IDENTIFIER ::= {id-at 81}

-- id-at-permission                             OBJECT IDENTIFIER  ::=  {id-at 82}
     X.509|Part8
-- Control  attributes
id-cat-sequenceMatchType OBJECT IDENTIFIER ::=
  {id-cat 1}

id-cat-wordMatchType OBJECT IDENTIFIER ::= {id-cat 2}

id-cat-characterMatchTypes OBJECT IDENTIFIER ::= {id-cat 3}

id-cat-selectedContexts OBJECT IDENTIFIER ::= {id-cat 4}

-- Notification attributes
id-not-dSAProblem OBJECT IDENTIFIER ::= {id-not 0}

id-not-searchServiceProblem OBJECT IDENTIFIER ::= {id-not 1}

id-not-serviceType OBJECT IDENTIFIER ::= {id-not 2}

id-not-attributeTypeList OBJECT IDENTIFIER ::= {id-not 3}

id-not-matchingRuleList OBJECT IDENTIFIER ::= {id-not 4}

id-not-filterItem OBJECT IDENTIFIER ::= {id-not 5}
```

```
id-not-attributeCombinations OBJECT IDENTIFIER ::= {id-not 6}

id-not-contextTypeList OBJECT IDENTIFIER ::= {id-not 7}

id-not-contextList OBJECT IDENTIFIER ::= {id-not 8}

id-not-contextCombinations OBJECT IDENTIFIER ::= {id-not 9}

id-not-hierarchySelectList OBJECT IDENTIFIER ::= {id-not 10}

id-not-searchControlOptionsList OBJECT IDENTIFIER ::= {id-not 11}

id-not-serviceControlOptionsList OBJECT IDENTIFIER ::= {id-not 12}

id-not-multipleMatchingLocalities OBJECT IDENTIFIER ::= {id-not 13}

id-not-proposedRelaxation OBJECT IDENTIFIER ::= {id-not 14}

id-not-appliedRelaxation OBJECT IDENTIFIER ::= {id-not 15}

-- Problem definitions
id-pr-targetDsaUnavailable OBJECT IDENTIFIER ::=
  {id-pr 1}

id-pr-dataSourceUnavailable OBJECT IDENTIFIER ::= {id-pr 2}

id-pr-unidentifiedOperation OBJECT IDENTIFIER ::= {id-pr 3}

id-pr-unavailableOperation OBJECT IDENTIFIER ::= {id-pr 4}

id-pr-searchAttributeViolation OBJECT IDENTIFIER ::= {id-pr 5}

id-pr-searchAttributeCombinationViolation OBJECT IDENTIFIER ::= {id-pr 6}

id-pr-searchValueNotAllowed OBJECT IDENTIFIER ::= {id-pr 7}

id-pr-missingSearchAttribute OBJECT IDENTIFIER ::= {id-pr 8}

id-pr-searchValueViolation OBJECT IDENTIFIER ::= {id-pr 9}

id-pr-attributeNegationViolation OBJECT IDENTIFIER ::= {id-pr 10}

id-pr-searchValueRequired OBJECT IDENTIFIER ::= {id-pr 11}

id-pr-invalidSearchValue OBJECT IDENTIFIER ::= {id-pr 12}

id-pr-searchContextViolation OBJECT IDENTIFIER ::= {id-pr 13}

id-pr-searchContextCombinationViolation OBJECT IDENTIFIER ::= {id-pr 14}

id-pr-missingSearchContext OBJECT IDENTIFIER ::= {id-pr 15}

id-pr-searchContextValueViolation OBJECT IDENTIFIER ::= {id-pr 16}

id-pr-searchContextValueRequired OBJECT IDENTIFIER ::= {id-pr 17}

id-pr-invalidContextSearchValue OBJECT IDENTIFIER ::= {id-pr 18}

id-pr-unsupportedMatchingRule OBJECT IDENTIFIER ::= {id-pr 19}

id-pr-attributeMatchingViolation OBJECT IDENTIFIER ::= {id-pr 20}

id-pr-unsupportedMatchingUse OBJECT IDENTIFIER ::= {id-pr 21}

id-pr-matchingUseViolation OBJECT IDENTIFIER ::= {id-pr 22}

id-pr-hierarchySelectForbidden OBJECT IDENTIFIER ::= {id-pr 23}
```

```
id-pr-invalidHierarchySelect OBJECT IDENTIFIER ::= {id-pr 24}

id-pr-unavailableHierarchySelect OBJECT IDENTIFIER ::= {id-pr 25}

id-pr-invalidSearchControlOptions OBJECT IDENTIFIER ::= {id-pr 26}

id-pr-invalidServiceControlOptions OBJECT IDENTIFIER ::= {id-pr 27}

id-pr-searchSubsetViolation OBJECT IDENTIFIER ::= {id-pr 28}

id-pr-unmatchedKeyAttributes OBJECT IDENTIFIER ::= {id-pr 29}

id-pr-ambiguousKeyAttributes OBJECT IDENTIFIER ::= {id-pr 30}

id-pr-unavailableRelaxationLevel OBJECT IDENTIFIER ::= {id-pr 31}

id-pr-emptyHierarchySelection OBJECT IDENTIFIER ::= {id-pr 32}

id-pr-administratorImposedLimit OBJECT IDENTIFIER ::= {id-pr 33}

id-pr-permanentRestriction OBJECT IDENTIFIER ::= {id-pr 34}

id-pr-temporaryRestriction OBJECT IDENTIFIER ::= {id-pr 35}

id-pr-relaxationNotSupported OBJECT IDENTIFIER ::= {id-pr 36}

-- Matching rules
-- id-mr-objectIdentifierMatch                    OBJECT IDENTIFIER  ::=  {id-mr 0}
     X.501|Part2
-- id-mr-distinguishedNameMatch               OBJECT IDENTIFIER  ::=  {id-mr 1}
     X.501|Part2
id-mr-caseIgnoreMatch OBJECT IDENTIFIER ::=
  {id-mr 2}

id-mr-caseIgnoreOrderingMatch OBJECT IDENTIFIER ::= {id-mr 3}

id-mr-caseIgnoreSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 4}

id-mr-caseExactMatch OBJECT IDENTIFIER ::= {id-mr 5}

id-mr-caseExactOrderingMatch OBJECT IDENTIFIER ::= {id-mr 6}

id-mr-caseExactSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 7}

id-mr-numericStringMatch OBJECT IDENTIFIER ::= {id-mr 8}

id-mr-numericStringOrderingMatch OBJECT IDENTIFIER ::= {id-mr 9}

id-mr-numericStringSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 10}

id-mr-caseIgnoreListMatch OBJECT IDENTIFIER ::= {id-mr 11}

id-mr-caseIgnoreListSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 12}

id-mr-booleanMatch OBJECT IDENTIFIER ::= {id-mr 13}

id-mr-integerMatch OBJECT IDENTIFIER ::= {id-mr 14}

id-mr-integerOrderingMatch OBJECT IDENTIFIER ::= {id-mr 15}

id-mr-bitStringMatch OBJECT IDENTIFIER ::= {id-mr 16}

id-mr-octetStringMatch OBJECT IDENTIFIER ::= {id-mr 17}

id-mr-octetStringOrderingMatch OBJECT IDENTIFIER ::= {id-mr 18}

id-mr-octetStringSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 19}
```

```
id-mr-telephoneNumberMatch OBJECT IDENTIFIER ::= {id-mr 20}

id-mr-telephoneNumberSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 21}

id-mr-presentationAddressMatch OBJECT IDENTIFIER ::= {id-mr 22}

id-mr-uniqueMemberMatch OBJECT IDENTIFIER ::= {id-mr 23}

id-mr-protocolInformationMatch OBJECT IDENTIFIER ::= {id-mr 24}

id-mr-uTCTimeMatch OBJECT IDENTIFIER ::= {id-mr 25}

id-mr-uTCTimeOrderingMatch OBJECT IDENTIFIER ::= {id-mr 26}

id-mr-generalizedTimeMatch OBJECT IDENTIFIER ::= {id-mr 27}

id-mr-generalizedTimeOrderingMatch OBJECT IDENTIFIER ::= {id-mr 28}

id-mr-integerFirstComponentMatch OBJECT IDENTIFIER ::= {id-mr 29}

id-mr-objectIdentifierFirstComponentMatch OBJECT IDENTIFIER ::= {id-mr 30}

id-mr-directoryStringFirstComponentMatch OBJECT IDENTIFIER ::= {id-mr 31}

id-mr-wordMatch OBJECT IDENTIFIER ::= {id-mr 32}

id-mr-keywordMatch OBJECT IDENTIFIER ::= {id-mr 33}

-- id-mr-certificateExactMatch                    OBJECT IDENTIFIER  ::=  {id-mr 34}
     X.509|Part8
-- id-mr-certificateMatch                         OBJECT IDENTIFIER  ::=  {id-mr 35}
     X.509|Part8
-- id-mr-certificatePairExactMatch                OBJECT IDENTIFIER  ::=  {id-mr 36}
     X.509|Part8
-- id-mr-certificatePairMatch                     OBJECT IDENTIFIER  ::=  {id-mr 37}
     X.509|Part8
-- id-mr-certificateListExactMatch                OBJECT IDENTIFIER  ::=  {id-mr 38}
     X.509|Part8
-- id-mr-certificateListMatch                     OBJECT IDENTIFIER  ::=  {id-mr 39}
     X.509|Part8
-- id-mr-algorithmIdentifierMatch             OBJECT IDENTIFIER  ::=  {id-mr 40}
     X.509|Part8
id-mr-storedPrefixMatch OBJECT IDENTIFIER ::=
  {id-mr 41}

-- id-mr-attributeCertificateMatch                OBJECT IDENTIFIER  ::=  {id-mr 42}
     X.509|Part8
-- id-mr-readerAndKeyIDMatch                  OBJECT IDENTIFIER  ::=  {id-mr 43}
-- id-mr-attributeIntegrityMatch                  OBJECT IDENTIFIER  ::=  {id-mr 44}
-- id-mr-attributeCertificateExactMatch           OBJECT IDENTIFIER  ::=  {id-mr 45}
     X.509|Part8
-- id-mr-holderIssuerMatch                    OBJECT IDENTIFIER  ::=  {id-mr 46}
     X.509|Part8
id-mr-systemProposedMatch OBJECT IDENTIFIER ::=
  {id-mr 47}

id-mr-generalWordMatch OBJECT IDENTIFIER ::= {id-mr 48}

id-mr-approximateStringMatch OBJECT IDENTIFIER ::= {id-mr 49}

id-mr-ignoreIfAbsentMatch OBJECT IDENTIFIER ::= {id-mr 50}

id-mr-nullMatch OBJECT IDENTIFIER ::= {id-mr 51}

id-mr-zonalMatch OBJECT IDENTIFIER ::= {id-mr 52}
```

```
-- id-mr-authAttIdMatch                        OBJECT IDENTIFIER  ::=  {id-mr 53}
     X.509|Part8
-- id-mr-roleSpecCertIdMatch                   OBJECT IDENTIFIER  ::=  {id-mr 54}
     X.509|Part8
-- id-mr-basicAttConstraintsMatch              OBJECT IDENTIFIER  ::=  {id-mr 55}
     X.509|Part8
-- id-mr-delegatedNameConstraintsMatch             OBJECT IDENTIFIER  ::=  {id-mr 56}
     X.509|Part8
-- id-mr-timeSpecMatch                         OBJECT IDENTIFIER  ::=  {id-mr 57}
     X.509|Part8
-- id-mr-attDescriptorMatch                    OBJECT IDENTIFIER  ::=  {id-mr 58}
     X.509|Part8
-- id-mr-acceptableCertPoliciesMatch               OBJECT IDENTIFIER  ::=  {id-mr 59}
     X.509|Part8
-- id-mr-policyMatch                           OBJECT IDENTIFIER  ::=  {id-mr 60}
     X.509|Part8
-- id-mr-delegationPathMatch                   OBJECT IDENTIFIER  ::=  {id-mr 61}
     X.509|Part8
-- id-mr-pkiPathMatch                          OBJECT IDENTIFIER  ::=  {id-mr 62}
     X.509|Part8
id-mr-facsimileNumberMatch OBJECT IDENTIFIER ::=
  {id-mr 63}

id-mr-facsimileNumberSubstringsMatch OBJECT IDENTIFIER ::= {id-mr 64}

-- id-mr-enhancedCertificateMatch              OBJECT IDENTIFIER  ::=  {id-mr 65}
     X.509|Part8
-- id-mr-sOAIdentifierMatch                    OBJECT IDENTIFIER  ::=  {id-mr 66}
     X.509|Part8
-- id-mr-extensionPresenceMatch                OBJECT IDENTIFIER  ::=  {id-mr 67}
     X.509|Part8
id-mr-uuidpairmatch OBJECT IDENTIFIER ::=
  {id-mr 68}

-- id-mr-dualStringMatch                       OBJECT IDENTIFIER  ::=  {id-mr 69}
     X.509|Part8
-- contexts
id-avc-language OBJECT IDENTIFIER ::=
  {id-avc 0}

id-avc-temporal OBJECT IDENTIFIER ::= {id-avc 1}

id-avc-locale OBJECT IDENTIFIER ::= {id-avc 2}

-- id-avc-attributeValueSecurityLabelContext        OBJECT IDENTIFIER  ::=  {id-avc 3}
-- id-avc-attributeValueIntegrityInfoContext            OBJECT IDENTIFIER  ::=  {id-avc
4}
id-avc-ldapAttributeOption OBJECT IDENTIFIER ::=
  {id-avc 5}

END -- SelectedAttributeTypes
```

Replace Annex G with:

Annex G

Tag-based applications as they relate to these Directory Specifications

(This annex does not form an integral part of this Recommendation | International Standard)

G.1 Introduction

ITU-T Rec. Y.2213 specifies the Next Generation Network (NGN) requirements and capabilities for applications and services using tag-based identification.

Tag-based applications and services are applications and services making use of tag-based identification, which is defined as the process of identifying a physical or logical object from other physical or logical objects by using identifiers stored on an ID tag. It involves accessing such ID tags and retrieving the associated information related to the identifier within the tag. The associated information may be a movie, information about a parcel, manufacture contact information, product specification, etc. ID tags can be Radio Frequency Identification (RFID), different types of bar codes, smart cards, etc.

Tag-based applications and services involve the following aspects:

a) *Identifier:* A series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g. physical or logical objects). Identifiers can be used for registration or authorization.

b) *ID tag:* A physical object that stores one or more identifiers and optionally application data such as name, title, price, address, etc.

c) *ID terminal*: A device with a data reading and optional writing capability which reads (and optionally writes) identifier(s) and possible application data from/to an ID tag.

d) *Associated information*: According to ITU-T Rec. Y.2213 this item is optional. However, this annex is concerned with how to get to such information.

This annex provides background material for how applications and services using tag-based identification may be supported by these Directory Specifications.

ITU-T Rec. Y.2213 specifies different levels of support:

a) Forward identifier resolution, which means resolving the identifier into associated information.

b) Reverse identifier resolution, which means resolving the associated information into the corresponding identifier.

c) One-to-many associations between an identifier and information of different types vs. one-to-one association. One-to-many associations allow users to access association information depending on the type of user. Manufacturers, retailers or consumers may access different types of associated information based on the same identifier.

NGN requires protection against a single point of failure.

The following describes how the above requirement may be supported using systems supporting these Directory Specifications. The capabilities used are primarily limited to those capabilities that are also supported by the LDAP specifications. When capabilities are required that go beyond the LDAP standard capabilities, it is clearly stated.

NOTE 1 – Use of LDAP based systems provides low-cost solutions.

The consideration in this annex is limited to frequency identification (RFID) based application and only those aspects of RFID that is covered by ISO/IEC 18000-3m3 and ISO/IEC 18000-6C.

Editor's note: Is the latter restriction necessary? The editor does not have access to the ISO/IEC 18000 series of documents.

NOTE 2 - Other types of tag-based applications may be added in the future.

G.2 Unique Item Identifier

A Unique Item Identifier (UII) is a common nomination for different types of identifiers used by tag-based applications.

ISO/IEC 18000-3m3 and ISO/IEC 18000-6C distinguish between two classes of UIIs:

a) Electronic Product Code (EPC) is a particular UII type developed by the EPCglobal organisation.

b) UII types defined within the context of International Standards and/or ITU-T Recommendations.

A particular bit (toggle bit) on the RFID tag indicates whether EPCglobal or ISO (which may mean ISO, ISO/IEC and/or ITU-T) provides the specification for the tag-content, including the UII format specification.

G.2.1 Electronic Product Code (EPC)

The EPC UII takes different forms such as the identity of a physical object for sale (SGTIN), a shipping container (SSCC), a returnable transport item (GRAI), an asset identifier (GIAI), a serialized location code (SGLN), a serialized service code (GSRN), or a serialized document number (GDTI).

The first eight bits of an EPC UII is the header and indicates the EPC UII type, although there is an escape mechanism that allows multi-octets headers to be defined in the future. An EPC UII is a series of bits with an implied hierarchical structure. As an example, some bits may denote a manufacturer; some other bits may denote a type of product; and some bits may be a serial number.

As an EPC can be divided into a series of components having a hierarchical relationship, it is possible to convert an EPC to a global unique Uniform Resource Name (URN). This is described in the Object Name Service (ONS) specification developed by EPCglobal. ONS resolves such URN into a pointer to the associated information. An ONS server is a Domain Name System (DNS) server dedicated to providing ONS.

The EPC format is specified by the Tag Data Standard issued by EPCglobal.

Editor's note – Currently this annex does not consider how EPC may be supported by these Directory Specifications.

G.2.2 ISO type tags

ISO type UIIs can only be assumed unique within a particular application. To ensure global uniqueness, each class of applications should be assigned an object identifier. Such object identifiers are typically allocated by international standards and/or assigned registration authorities. Together, the (object identifier; UII) tuple uniquely identify an object. G.3 provides examples of object identifier structures.

An ISO tag also includes a field called Application Family Identifier (AFI). It is a one-octet field, although there is an escape mechanism to provide multiple-octets AFIs in the future. Several AFIs may be associated with the same object identifier, but a single AFI is not associated with multiple object identifiers. In the case, the object identifier is not available; the object identifier can in principle be deduced from the AFI.

Editor's note – At least this is the understanding of the editor.

G.3 Object identifier use by RFID applications

Figure G.1 shows examples of object identifier applications. Object identifiers, or at least the upper level arcs, are allocated by International Standards and/or ITU-T Recommendations. As an example, ISO/IEC 15961 defines the top level arcs as listed below.

- {1 0 15961 8} is an object identifier for data format used for libraries according to ISO/IEC 28560-2 "Information and documentation -- RFID in libraries -- Part 2: Encoding based on ISO/IEC 15962"
- {1 0 15961 9} is an object identifier for data format used when all the data on the RFID tag complies with the EAN.UCC System (EAN International and Uniform Code Council), as referred to in ISO/IEC 15418 "Information technology -- EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance"
- {1 0 15961 10} is an object identifier for data format used when all the data on the RFID tag complies with the Data Identifier standard (as referred to in ISO/IEC 15418).
- {1 0 15961 11} is an object identifier for the Universal Postal Union.
- {1 0 15961 12} is the object identifier for International Air Transport Association (IATA). IATA may further define sub-arcs for specific purposes. As an example, sub-arc 1 is used for IATA Baggage Identification Code.

ITU-T Rec. X.668 | ISO/IEC 9834-9 specifies an object identifier structure to be used by tag-based applications. It defines a structure requiring only three arcs to save storage on RFID tags. New RFID applications may choose to apply for an arc within this structure. Current applications may choose to convert to this object identifier structure. ITU-T Rec. Y.2213 requires support of this object identifier structure.

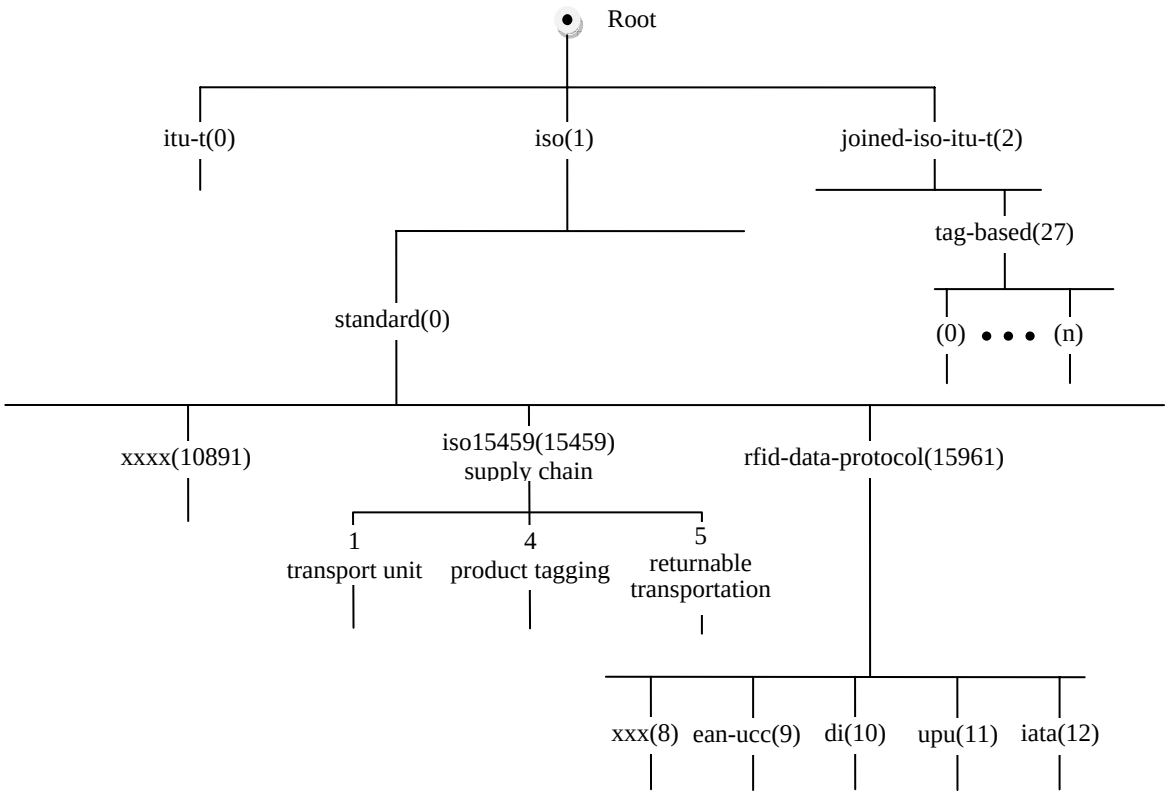

Figure G.1 – RFID object identifier structure

G.4 RFID support by use of directory technology

Directory, as defined by these Directory Specifications or by LDAP, provides efficient support for RFID-based applications:

- By use of off-the-shelf software.
- Use of well known technology.
- A single access allows retrieval of the information associated with an RFID tag or it allows retrieving a URL for the associated information.
- It is not necessary to convert the UII to URN format.
- Possibility for return of diverse and complex data structures.
- Extensive security functions.

The RFID reader or its associated equipment (e.g. a PC) must support either the LDAP or the DAP protocol.

G.5 Forward identifier resolution

G.5.1 Search using the (object identifier; UII) tuple

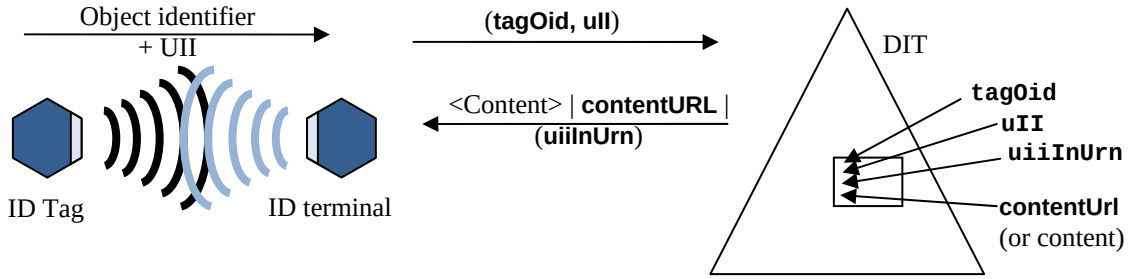

Figure G.2 – ID terminal using combined search

Figure G.2 illustrates the case where an ID terminal reads the RFID tag to get the object identifier and the UII. The tuple (object identifier, UII) are forwarded in the filter of a search request. The search will locate the entry that holds those two values in the attribute of type **tagOid** and the attribute of type **uII**, respectively. This entry may hold either the content associated with the RFID tag or it may hold a URL in a **contentUrl** attribute pointing to the location where the content might be found. Alternative a pointer to another directory location may provided in the form of a referral, e.g. to another LDAP server.

The contents can take many shapes. It may be necessary to defined application specific attribute types to hold the content. The content may be spread over several attributes of different types. Some content information may also be carried by existing attribute types, such a postal address, telephone number, web address, etc.

If for some reason, the UII is wanted in URN format, such an URN could be provided in an attribute of type **uiiInURN**.

G.5.2 Search using the (AFI; UII) tuple

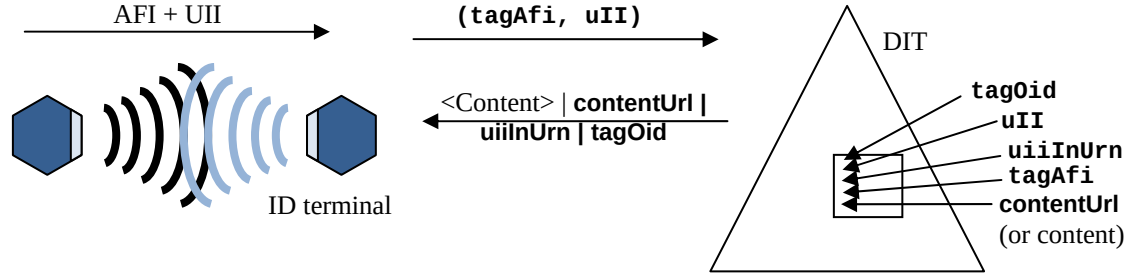

Figure G.3 – Retrieval of information using AFI an UII values

If an object identifier is not available on the tag, the AFI may be used instead if the relevant entry holds an attribute of type **tagAfi** holding the AFI(s) associated with the relevant object identifier. This object identifier may be held by an attribute of type **tagOid**. The AFI and the UII together will locate required information, as indicated in G.5.1.

G.5.3 Retrieving UII format information

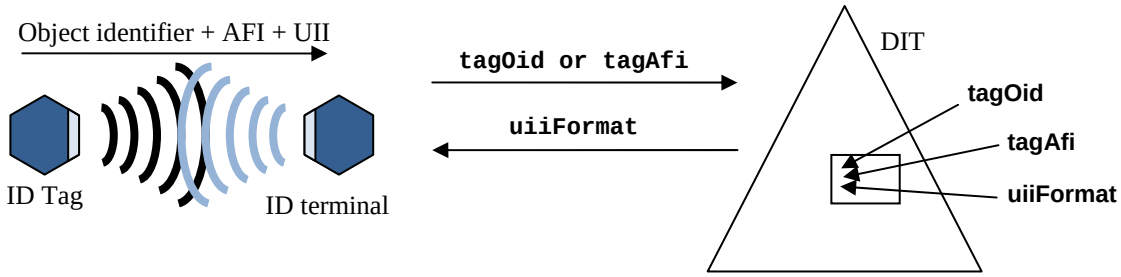

Figure G.4 – Retrieving UII format information

The ID terminal may access the Directory to retrieve UII format information. Figure G.4 illustrates that. An attribute of type **uiiFormat** may hold this information.

The ID terminal may use this information to truncate the UII to get, as an example, information about the manufacturer or the type of object rather than information about the instant of object as identified by the complete UII.

The ID terminal may also construct a global unique URN representation of the UII if the **urnPrefix** component is included in the attribute value.

NOTE – There is no need for the sake of accessing the Directory to transform to a URN representation.

G.5.3 Use of special DIT subtree structure

Alternatively, a DIT structure as discussed in G.8 may be utilized. Here the relevant attributes may be placed in an entry of the object classes **oidCobj**. The tag object identifier may then be mapped directly into a distinguished name and the attributes may be retrieved by a Read operation.

NOTE – LDAP does not have a Read operation, but can imitate a Read operation using a special Search operation

G.6 Information association types

In the simple case above, there is a one-to-one relationship between a tag and its associated information. However, there are cases where there are several sources of information associated with a single tag and there are cases where multiple tags are associated with the same information.

G.6.1 Information associated with truncated UII

In addition to the information associated with the complete UII, there may be other type of information related to truncated UIIs as indicated in G.5.3. This is an example of a many-to-one relationship between identifier and a single source of information.

G.6.2 Multiple user groups for single tag

Different user groups may require different associated information even for the same UII or the same truncated UII. For example, manufacturers may use identifiers for production planning while retailers may use the same identifiers for store inventory management, and consumers may use the same identifiers for product information retrieval. There are different ways this may be achieved:

- Use of access control: Different contents may be held by different attributes. By use of access control, a particular user group will only get access to information relevant for that user group. Likewise, if the returned information is a URL to the content, different URLs may be held by the same attribute. By use of access control down to value level, only the relevant URL will be returned.

  NOTE 1 – LDAP does not have access control specifications, although many LDAP implementations have proprietary access control implementations.

- Different user groups may access different directory systems. This will require that some information is duplicated among these systems.
- Use of contexts *(more text here)*.

  NOTE 2 – Context is not supported by LDAP

- Use of service administration *(more text here)*.

NOTE 3 – Service administration is not supported by LDAP

G.7 Reverse identifier resolution

7.2 of ITU-T Rec. Y.2213 specifies a requirement for reverse resolution i.e., finding the identifier of an object and its location from the associated information. Reverse identification only makes sense if the associated information is only relevant for a single identifier.

If the Directory provides the associated information, the entry holding that information may also hold attributes of **tagOid** and **uII** attribute types holding the required information. If the directory does not provide the associated information, the identity information may be provided in the entry that holds the URL of that information.

G.7 Location information

7.6 of ITU-T Rec. Y.2213 specifies a requirement for location-based service support.

The location of tag may be provided in an attribute of type **tagLocation**. This attribute may be maintained by the ID terminal or by off-line means.

Editor's note – Is there a requirement for an attribute type for ID terminal location?

Editor's note – Can we imagine services depending on the location of the tag?

G.8 DIT structure for entries representing object identifier components

An object identifier structure may be represented by one or more DIT subtrees. Each arc of the object identifier structure is represented by a directory entry. A first level arc is represented by an entry of object class **oidC1obj**. A second level arc is represented by an entry of object class **oidC2obj**, while all lower level arcs are represented by entries of object class **oidCobj**. ITU-T Rec. X.521 | ISO/IEC 9594-7 defines these object classes.

An entry representing an object identifier arc shall have an RDN with a numeric value equal the numeric value assigned to the object identifier arc. The attribute types used for RDN are defined in ITU-T Rec. X.660 | ISO/IEC 9834-1. An entry of the **oidC1obj** object class and shall hold an attribute of type **oidC1** and have the value 0, 1 or 2 depending on the type of top-level arc. An entry of the **oidC2obj** object class and shall hold an attribute of type **oidC2**. An entry of the **oidCobj** object class and shall hold an attribute of type **oidC**.

An object identifier allocated according to ITU-T Rec. X.668 | ISO/IEC 9834-9 specifies that the top-level arc shall be the one allocated to common ITU-T and ISO/IEC use. This means that in a tag-based environment based on this object identifier structure, the attribute of type **oidC1** shall have the value 2 and the attribute of type **oidC2** shall have the value 27.

For object identifiers allocated according ISO standards, an attribute of type **oidC1** shall have the value 1 and an attribute of type **oidC2** shall have the value 0.

Figure G.5 shows two DIT subtrees representing the object identifier structure shown in figure G.1. These subtrees could in principle be anywhere within the DIT, but if an ID terminal accesses information in this subtree, as discussed in G.5.3, a Read operation will be simplified if the object identifier subtree is just below the DIT root as indicated in the figure.

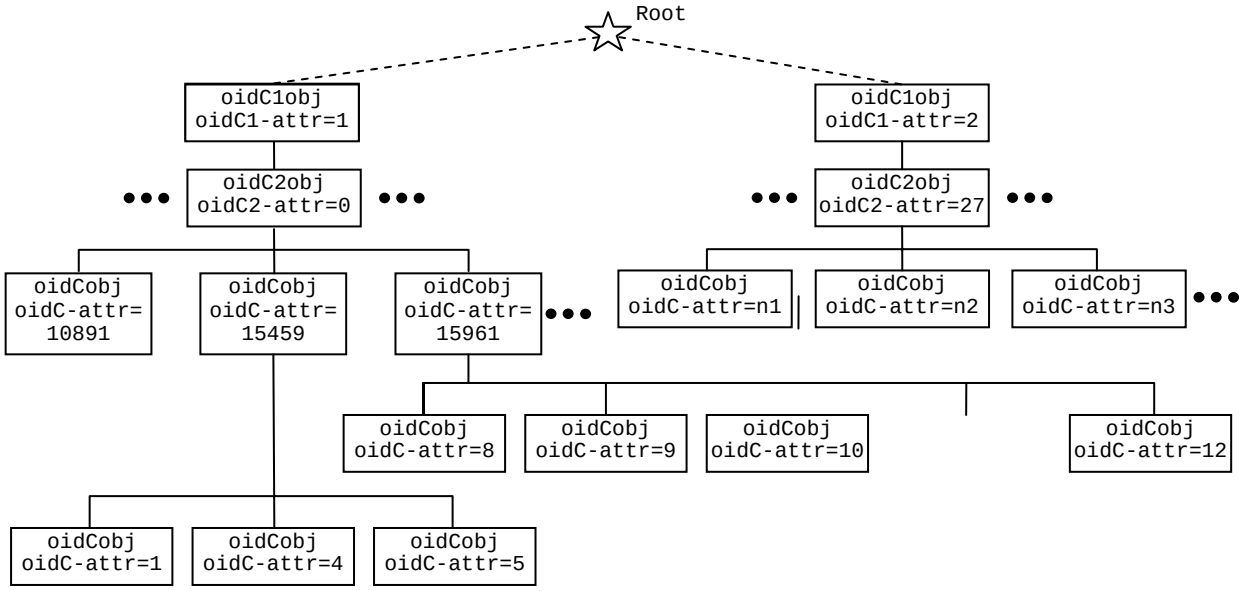

Figure G.5 – Possible DIT subtree representing object identifier components in a tag-based environment

ISO/IEC 9594-7 : 2008, Information Technology - Open systems Interconnection - The Directory: Selected Object Classes

Working draft for Amendment 1: Communications support enhancements

Update the ASN.1 of 6.23 as shown

```
tagInformation  OBJECT-CLASS  ::=  {
  SUBCLASS OF  { top }
  KIND         auxiliary
  MAY CONTAIN  { tagOid |
                 tagAfi |
                 uii |
                 uiiFormat |
                 uiiInUrn |
                 contentUrl |
                 tagLocation }
  ID           id-oc-tagInformation }
```

Annex A

Selected object classes and name forms in ASN.1

Replace the ASN.1 module in Annex A with the following

```
SelectedObjectClasses {joint-iso-itu-t ds(5) module(1) selectedObjectClasses(6)
  6} DEFINITIONS ::=
BEGIN

--  EXPORTS All
```

```
--  The types and values defined in this module are exported for use in the other ASN.1
modules contained
--  within the Directory Specifications, and for the use of other applications which will
use them to access
--  Directory services. Other applications may use them for their own purposes, but this
will not constrain
--  extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  authenticationFramework, certificateExtensions, id-nf, id-oc,
    informationFramework, objectClass, selectedAttributeTypes
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  alias, ATTRIBUTE, NAME-FORM, OBJECT-CLASS, top
    FROM InformationFramework informationFramework
  -- from ITU-T Rec. X.520 | ISO/IEC 9594-6
  businessCategory, commonName, contentUri, countryName, description,
    destinationIndicator, dmdName, facsimileTelephoneNumber,
    internationalISDNNumber, knowledgeInformation, localityName, member,
    organizationalUnitName, organizationName, owner,
    physicalDeliveryOfficeName, postalAddress, postalCode, postOfficeBox,
    preferredDeliveryMethod, presentationAddress, registeredAddress,
    roleOccupant, searchGuide, seeAlso, serialNumber, stateOrProvinceName,
    streetAddress, supportedApplicationContext, surname, tagOid,
    telephoneNumber, telexNumber, title, uiiFormat, uiiInUrn, uniqueMember,
    x121Address
    FROM SelectedAttributeTypes selectedAttributeTypes
  -- from ITU-T Rec. X.509 | ISO/IEC 9594-8
  authorityRevocationList, cACertificate, certificateRevocationList,
    crossCertificatePair, deltaRevocationList, supportedAlgorithms,
    userCertificate, userPassword
    FROM AuthenticationFramework authenticationFramework
  -- from ITU-T Rec. X.660 | ISO/IEC 9834-1
  oidC, oidC1, oidC2
    FROM OidDirectoryNameDef {joint-iso-itu-t registration-procedures(17)
      module(1) oidDirectoryNameDef(1)};

--  Attribute sets
TelecommunicationAttributeSet ATTRIBUTE ::=
  {facsimileTelephoneNumber | internationalISDNNumber | telephoneNumber |
    --    teletexTerminalIdentifier | Attribute type has been deleted
   telexNumber | preferredDeliveryMethod | destinationIndicator |
   registeredAddress | x121Address}

PostalAttributeSet ATTRIBUTE ::=
  {physicalDeliveryOfficeName | postalAddress | postalCode | postOfficeBox |
   streetAddress}

LocaleAttributeSet ATTRIBUTE ::=
  {localityName | stateOrProvinceName | streetAddress}

OrganizationalAttributeSet ATTRIBUTE ::=
  {description | LocaleAttributeSet | PostalAttributeSet |
   TelecommunicationAttributeSet | businessCategory | seeAlso | searchGuide |
   userPassword}

--  Object classes
country OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {countryName}
  MAY CONTAIN   {description | searchGuide}
  ID            id-oc-country
}

locality OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  MAY CONTAIN  {description | searchGuide | LocaleAttributeSet | seeAlso}
  ID           id-oc-locality
```

```
}

organization OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {organizationName}
  MAY CONTAIN   {OrganizationalAttributeSet}
  ID            id-oc-organization
}

organizationalUnit OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {organizationalUnitName}
  MAY CONTAIN   {OrganizationalAttributeSet}
  ID            id-oc-organizationalUnit
}

person OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName | surname}
  MAY CONTAIN   {description | telephoneNumber | userPassword | seeAlso}
  ID            id-oc-person
}

organizationalPerson OBJECT-CLASS ::= {
  SUBCLASS OF  {person}
  MAY CONTAIN
    {LocaleAttributeSet | PostalAttributeSet | TelecommunicationAttributeSet |
      organizationalUnitName | title}
  ID           id-oc-organizationalPerson
}

organizationalRole OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName}
  MAY CONTAIN
    {description | LocaleAttributeSet | organizationalUnitName |
      PostalAttributeSet | preferredDeliveryMethod | roleOccupant | seeAlso |
      TelecommunicationAttributeSet}
  ID            id-oc-organizationalRole
}

groupOfNames OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName | member}
  MAY CONTAIN
    {description | organizationName | organizationalUnitName | owner | seeAlso
      | businessCategory}
  ID            id-oc-groupOfNames
}

groupOfUniqueNames OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName | uniqueMember}
  MAY CONTAIN
    {description | organizationName | organizationalUnitName | owner | seeAlso
      | businessCategory}
  ID            id-oc-groupOfUniqueNames
}

residentialPerson OBJECT-CLASS ::= {
  SUBCLASS OF   {person}
  MUST CONTAIN  {localityName}
  MAY CONTAIN
    {LocaleAttributeSet | PostalAttributeSet | preferredDeliveryMethod |
      TelecommunicationAttributeSet | businessCategory}
  ID            id-oc-residentialPerson
}
```

```
applicationProcess OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName}
  MAY CONTAIN   {description | localityName | organizationalUnitName | seeAlso}
  ID            id-oc-applicationProcess
}

applicationEntity OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName | presentationAddress}
  MAY CONTAIN
    {description | localityName | organizationName | organizationalUnitName |
      seeAlso | supportedApplicationContext}
  ID            id-oc-applicationEntity
}

dSA OBJECT-CLASS ::= {
  SUBCLASS OF  {applicationEntity}
  MAY CONTAIN  {knowledgeInformation}
  ID           id-oc-dSA
}

device OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {commonName}
  MAY CONTAIN
    {description | localityName | organizationName | organizationalUnitName |
      owner | seeAlso | serialNumber}
  ID            id-oc-device
}

strongAuthenticationUser OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          auxiliary
  MUST CONTAIN  {userCertificate}
  ID            id-oc-strongAuthenticationUser
}

userSecurityInformation OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {supportedAlgorithms}
  ID           id-oc-userSecurityInformation
}

certificationAuthority OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          auxiliary
  MUST CONTAIN
    {cACertificate | certificateRevocationList | authorityRevocationList}
  MAY CONTAIN   {crossCertificatePair}
  ID            id-oc-certificationAuthority
}

certificationAuthority-V2 OBJECT-CLASS ::= {
  SUBCLASS OF  {certificationAuthority}
  KIND         auxiliary
  MAY CONTAIN  {deltaRevocationList}
  ID           id-oc-certificationAuthority-V2
}

dMD OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {dmdName}
  MAY CONTAIN   {OrganizationalAttributeSet}
  ID            id-oc-dmd
}
```

```
oidC1obj OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {oidC1}
  ID            id-oc-oidC1obj
}

oidC2obj OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {oidC2}
  ID            id-oc-oidC2obj
}

oidCobj OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  MUST CONTAIN  {oidC}
  ID            id-oc-oidCobj
}

uiiToUrn OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          auxiliary
  MUST CONTAIN  {uiiFormat}
  MAY CONTAIN   {tagOid}
  ID            id-oc-uiiToUrn
}

urnToUrl OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          auxiliary
  MUST CONTAIN  {uiiInUrn | contentUri}
  MAY CONTAIN   {tagOid}
  ID            id-oc-urnToUri
}

--  Name forms
countryNameForm NAME-FORM ::= {
  NAMES            country
  WITH ATTRIBUTES  {countryName}
  ID               id-nf-countryNameForm
}

locNameForm NAME-FORM ::= {
  NAMES            locality
  WITH ATTRIBUTES  {localityName}
  ID               id-nf-locNameForm
}

sOPNameForm NAME-FORM ::= {
  NAMES            locality
  WITH ATTRIBUTES  {stateOrProvinceName}
  ID               id-nf-sOPNameForm
}

orgNameForm NAME-FORM ::= {
  NAMES            organization
  WITH ATTRIBUTES  {organizationName}
  ID               id-nf-orgNameForm
}

orgUnitNameForm NAME-FORM ::= {
  NAMES            organizationalUnit
  WITH ATTRIBUTES  {organizationalUnitName}
  ID               id-nf-orgUnitNameForm
}

personNameForm NAME-FORM ::= {
  NAMES            person
  WITH ATTRIBUTES  {commonName}
```

```
  ID               id-nf-personNameForm
}

orgPersonNameForm NAME-FORM ::= {
  NAMES            organizationalPerson
  WITH ATTRIBUTES  {commonName}
  AND OPTIONALLY   {organizationalUnitName}
  ID               id-nf-orgPersonNameForm
}

orgRoleNameForm NAME-FORM ::= {
  NAMES            organizationalRole
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-orgRoleNameForm
}

gONNameForm NAME-FORM ::= {
  NAMES            groupOfNames
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-gONNameForm
}

resPersonNameForm NAME-FORM ::= {
  NAMES            residentialPerson
  WITH ATTRIBUTES  {commonName}
  AND OPTIONALLY   {streetAddress}
  ID               id-nf-resPersonNameForm
}

applProcessNameForm NAME-FORM ::= {
  NAMES            applicationProcess
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-applProcessNameForm
}

applEntityNameForm NAME-FORM ::= {
  NAMES            applicationEntity
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-applEntityNameForm
}

dSANameForm NAME-FORM ::= {
  NAMES            dSA
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-dSANameForm
}

deviceNameForm NAME-FORM ::= {
  NAMES            device
  WITH ATTRIBUTES  {commonName}
  ID               id-nf-deviceNameForm
}

dMDNameForm NAME-FORM ::= {
  NAMES            dMD
  WITH ATTRIBUTES  {dmdName}
  ID               id-nf-dMDNameForm
}

oidC1NameForm NAME-FORM ::= {
  NAMES            oidC1obj
  WITH ATTRIBUTES  {oidC1}
  ID               id-nf-oidC1NameForm
}

oidC2NameForm NAME-FORM ::= {
  NAMES            oidC2obj
  WITH ATTRIBUTES  {oidC2}
```

```
  ID               id-nf-oidC2NameForm
}

oidCNameForm NAME-FORM ::= {
  NAMES            oidCobj
  WITH ATTRIBUTES  {oidC}
  ID               id-nf-oidCNameForm
}

--  Object identifier assignments
--  object identifiers assigned in other modules are shown in comments
--  Object classes
--  id-oc-top                   OBJECT IDENTIFIER  ::=  {id-oc 0} Defined in ITU-T Rec.
X.501 |
--                                                          ISO/IEC 9594-2
--  id-oc-alias                 OBJECT IDENTIFIER  ::=  {id-oc 1} Defined in ITU-T Rec.
X.501 |
--                                                          ISO/IEC 9594-2
id-oc-country OBJECT IDENTIFIER ::=
  {id-oc 2}

id-oc-locality OBJECT IDENTIFIER ::= {id-oc 3}

id-oc-organization OBJECT IDENTIFIER ::= {id-oc 4}

id-oc-organizationalUnit OBJECT IDENTIFIER ::= {id-oc 5}

id-oc-person OBJECT IDENTIFIER ::= {id-oc 6}

id-oc-organizationalPerson OBJECT IDENTIFIER ::= {id-oc 7}

id-oc-organizationalRole OBJECT IDENTIFIER ::= {id-oc 8}

id-oc-groupOfNames OBJECT IDENTIFIER ::= {id-oc 9}

id-oc-residentialPerson OBJECT IDENTIFIER ::= {id-oc 10}

id-oc-applicationProcess OBJECT IDENTIFIER ::= {id-oc 11}

id-oc-applicationEntity OBJECT IDENTIFIER ::= {id-oc 12}

id-oc-dSA OBJECT IDENTIFIER ::= {id-oc 13}

id-oc-device OBJECT IDENTIFIER ::= {id-oc 14}

id-oc-strongAuthenticationUser OBJECT IDENTIFIER ::=
  {id-oc 15} -- Deprecated, see 6.15

id-oc-certificationAuthority OBJECT IDENTIFIER ::=
  {id-oc 16} -- Deprecated, see 6.17

id-oc-certificationAuthority-V2 OBJECT IDENTIFIER ::=
  {id-oc 16 2} -- Deprecated, see 6.18

id-oc-groupOfUniqueNames OBJECT IDENTIFIER ::= {id-oc 17}

id-oc-userSecurityInformation OBJECT IDENTIFIER ::= {id-oc 18}

-- id-oc-cRLDistributionPoint         OBJECT IDENTIFIER  ::=  {id-oc 19}    Defined in
ITU-T Rec. X.509 |
--                                                          ISO/IEC 9594-8
id-oc-dmd OBJECT IDENTIFIER ::=
  {id-oc 20}

-- id-oc-pkiUser                 OBJECT IDENTIFIER  ::=  {id-oc 21}    Defined in ITU-T
Rec. X.509 |
--                                                          ISO/IEC 9594-8
```

```
-- id-oc-pkiCA              OBJECT IDENTIFIER  ::=  {id-oc 22}    Defined in ITU-T Rec.
X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-deltaCRL                OBJECT IDENTIFIER  ::=  {id-oc 23}    Defined in ITU-T
Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-pmiUser                 OBJECT IDENTIFIER  ::=  {id-oc 24}    Defined in ITU-T
Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-pmiAA              OBJECT IDENTIFIER  ::=  {id-oc 25}    Defined in ITU-T Rec.
X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-pmiSOA                  OBJECT IDENTIFIER  ::=  {id-oc 26}    Defined in ITU-T
Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-attCertCRLDistributionPts    OBJECT IDENTIFIER  ::=  {id-oc 27}    Defined in
ITU-T Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-parent                  OBJECT IDENTIFIER  ::=  {id-oc 28}    Defined in ITU-T
Rec. X.501 |
--                                                                 ISO/IEC 9594-2
-- id-oc-child                   OBJECT IDENTIFIER  ::=  {id-oc 29}    Defined in ITU-T
Rec. X.501 |
--                                                                 ISO/IEC 9594-2
-- id-oc-cpCps              OBJECT IDENTIFIER  ::=  {id-oc 30}    Defined in ITU-T Rec.
X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-pkiCertPath             OBJECT IDENTIFIER  ::=  {id-oc 31}    Defined in ITU-T
Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-privilegePolicy              OBJECT IDENTIFIER  ::=  {id-oc 32}    Defined in
ITU-T Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-pmiDelegationPath       OBJECT IDENTIFIER  ::=  {id-oc 33}    Defined in ITU-T
Rec. X.509 |
--                                                                 ISO/IEC 9594-8
-- id-oc-protectedPrivilegePolicy     OBJECT IDENTIFIER  ::=   {id-oc 34}   Defined in
ITU-T Rec. X.509 |
--                                                                 ISO/IEC 9594-8
id-oc-oidC1obj OBJECT IDENTIFIER ::=
  {id-oc 35}

id-oc-oidC2obj OBJECT IDENTIFIER ::= {id-oc 36}

id-oc-oidCobj OBJECT IDENTIFIER ::= {id-oc 37}

id-oc-uiiToUrn OBJECT IDENTIFIER ::= {id-oc 38}

id-oc-urnToUri OBJECT IDENTIFIER ::= {id-oc 39}

-- id-oc-integrityInfo           OBJECT IDENTIFIER  ::=   {id-oc 40}   Defined in ITU-T
Rec. X.501 |
--                                                                 ISO/IEC 9594-2
--  Name forms
id-nf-countryNameForm OBJECT IDENTIFIER ::=
  {id-nf 0}

id-nf-locNameForm OBJECT IDENTIFIER ::= {id-nf 1}

id-nf-sOPNameForm OBJECT IDENTIFIER ::= {id-nf 2}

id-nf-orgNameForm OBJECT IDENTIFIER ::= {id-nf 3}

id-nf-orgUnitNameForm OBJECT IDENTIFIER ::= {id-nf 4}

id-nf-personNameForm OBJECT IDENTIFIER ::= {id-nf 5}

id-nf-orgPersonNameForm OBJECT IDENTIFIER ::= {id-nf 6}
```

```
id-nf-orgRoleNameForm OBJECT IDENTIFIER ::= {id-nf 7}

id-nf-gONNameForm OBJECT IDENTIFIER ::= {id-nf 8}

id-nf-resPersonNameForm OBJECT IDENTIFIER ::= {id-nf 9}

id-nf-applProcessNameForm OBJECT IDENTIFIER ::= {id-nf 10}

id-nf-applEntityNameForm OBJECT IDENTIFIER ::= {id-nf 11}

id-nf-dSANameForm OBJECT IDENTIFIER ::= {id-nf 12}

id-nf-deviceNameForm OBJECT IDENTIFIER ::= {id-nf 13}

-- id-nf-cRLDistPtNameForm       OBJECT IDENTIFIER  ::=  {id-nf 14}
id-nf-dMDNameForm OBJECT IDENTIFIER ::=
  {id-nf 15}

-- id-nf-subentryNameForm        OBJECT IDENTIFIER  ::=  {id-nf 16}
id-nf-oidC1NameForm OBJECT IDENTIFIER ::=
  {id-nf 17}

id-nf-oidC2NameForm OBJECT IDENTIFIER ::= {id-nf 18}

id-nf-oidCNameForm OBJECT IDENTIFIER ::= {id-nf 19}

END -- SelectedObjectClasses
```

ISO/IEC 9594-8 : 2008, Information Technology - Open systems Interconnection - The Directory: Public-key and attribute certificate frameworks

Working draft for Amendment 1: Communications support enhancements

3.4.19 certification path: An ordered sequence of public-key certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

In clause 7, make the following additions:

a) Add at the top right after the level 1 header:

7.1 Introduction

b) Right after NOTE 1, add:

7.2 Public-key certificates

c) Right after NOTE 3, add:

7.3 Public-key certificate extensions

*d) Move the **ALGORITHM** information object class specification to right after the **SupportedAlgorithms** data type defintion:*

e) Right after the EXTENSION information object class, add:

7.4 Types of public-key certificates

f) Just before the paragraph starting with If user A, trying to obtain the public key of user B …,*add:*

7.5 Certification path

g) Just before the current second level 2 header 7.1 Generation of key pairs, *add*:

7.6 Trust anchors and root-CAs

Concept A is the "relative" or "relying party" viewpoint. Concept B is the "absolute" or "certification infrastructure" viewpoint. The fact that they are different concepts can be demonstrated by the simplest PKI example - a single hierarchical PKI where relying parties trust some, but not all, intermediate CAs. "Root CA" cannot be a synonym for "Trust Anchor" because RPs do configure intermediate CA certificates as TAs and do not configure the Root CA certificate as a TA.

In more complex PK Infrastructures such as cross-certified and bridge environments, the meaning of Root CA becomes fuzzier, while the meaning of TA remains solid - every application MUST have one or more TAs. In a meshed PKI (PGP, or Entrust's "trust begins at home"), the concept of a Root CA disappears entirely, yet applications still must have TAs.

h) renumber the second level headers accordingly.

Annex A

Public-Key and Attribute Certificate Frameworks

Replace the ASN.1 modules in Annex A with the following

```
AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
  authenticationFramework(7) 6} DEFINITIONS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- Directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
IMPORTS
  id-at, id-nf, id-oc, informationFramework, selectedAttributeTypes,
    basicAccessControl, certificateExtensions
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
```

```
      usefulDefinitions(0) 6}
  Name, ATTRIBUTE, OBJECT-CLASS, NAME-FORM, top
    FROM InformationFramework informationFramework
  UniqueIdentifier, octetStringMatch, commonName, UnboundedDirectoryString
    FROM SelectedAttributeTypes selectedAttributeTypes
  certificateExactMatch, certificatePairExactMatch, certificateListExactMatch,
    KeyUsage, GeneralNames, CertificatePoliciesSyntax,
    algorithmIdentifierMatch, CertPolicyId
    FROM CertificateExtensions certificateExtensions;

-- parameterized types
ENCRYPTED{ToBeEnciphered} ::=
  BIT STRING
    (CONSTRAINED BY {
       -- shall be the result of applying an encipherment procedure
       -- to the BER-encoded octets of a value of --ToBeEnciphered})

HASH{ToBeHashed} ::= SEQUENCE {
  algorithmIdentifier  AlgorithmIdentifier{{SupportedAlgorithms}},
  hashValue
    BIT STRING
      (CONSTRAINED BY {
         -- shall be the result of applying a hashing procedure to the DER-encoded octets
         -- of a value of -- ToBeHashed}),
  ...
}

ENCRYPTED-HASH{ToBeSigned} ::=
  BIT STRING
    (CONSTRAINED BY {
       -- shall be the result of applying a hashing procedure to the DER-encoded (see
6.1) octets
       -- of a value of --ToBeSigned -- and then applying an encipherment procedure to
those octets --})

SIGNATURE{ToBeSigned} ::= SEQUENCE {
  algorithmIdentifier  AlgorithmIdentifier{{SupportedAlgorithms}},
  encrypted            ENCRYPTED-HASH{ToBeSigned},
  ...
}

SIGNED{ToBeSigned} ::= SEQUENCE {
  toBeSigned  ToBeSigned,
  COMPONENTS OF SIGNATURE{ToBeSigned},
  ...
}

-- public-key certificate definition
Certificate ::= SIGNED{CertificateContent}

CertificateContent ::= SEQUENCE {
  version                 [0]  Version DEFAULT v1,
  serialNumber            CertificateSerialNumber,
  signature               AlgorithmIdentifier{{SupportedAlgorithms}},
  issuer                  Name,
  validity                Validity,
  subject                 Name,
  subjectPublicKeyInfo    SubjectPublicKeyInfo,
  issuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier OPTIONAL,
  ...,
  [[2: -- if present, version shall be v2 or v3
  subjectUniqueIdentifier  [2] IMPLICIT UniqueIdentifier OPTIONAL]],
  [[3: -- if present, version shall be v2 or v3
  extensions              [3]  Extensions OPTIONAL]]
  -- If present, version shall be v3]]
}

Version ::= INTEGER {v1(0), v2(1), v3(2)}
```

```
CertificateSerialNumber ::= INTEGER

AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm   ALGORITHM.&id({SupportedAlgorithms}),
  parameters  ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ...
}

-- Definition of the following information object set is deferred, perhaps to
standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the parameters component of AlgorithmIdentifier.
SupportedAlgorithms ALGORITHM ::=
  {...}

Validity ::= SEQUENCE {notBefore  Time,
                       notAfter   Time,
                       ...
}

SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm         AlgorithmIdentifier{{SupportedAlgorithms}},
  subjectPublicKey  BIT STRING,
  ...
}

Time ::= CHOICE {utcTime          UTCTime,
                 generalizedTime  GeneralizedTime
}

Extensions ::= SEQUENCE OF Extension

-- For those extensions where ordering of individual extensions within the SEQUENCE is
significant, the
-- specification of those individual extensions shall include the rules for the
significance of the order therein
Extension ::= SEQUENCE {
  extnId     EXTENSION.&id({ExtensionSet}),
  critical   BOOLEAN DEFAULT FALSE,
  extnValue
    OCTET STRING
      (CONTAINING EXTENSION.&ExtnType({ExtensionSet}{@extnId})
       ENCODED BY
       der),
  ...
}

der OBJECT IDENTIFIER ::=
  {joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1)}

ExtensionSet EXTENSION ::=
  {...}

EXTENSION ::= CLASS {&id        OBJECT IDENTIFIER UNIQUE,
                     &ExtnType
}WITH SYNTAX {SYNTAX &ExtnType
              IDENTIFIED BY &id
}

ALGORITHM ::= CLASS {&Type  OPTIONAL,
                     &id    OBJECT IDENTIFIER UNIQUE
}WITH SYNTAX {[&Type]
              IDENTIFIED BY &id
}

-- other PKI certificate constructs
Certificates ::= SEQUENCE {
```

```
  userCertificate    Certificate,
  certificationPath  ForwardCertificationPath OPTIONAL,
  ...
}

CertificationPath ::= SEQUENCE {
  userCertificate    Certificate,
  theCACertificates  SEQUENCE OF CertificatePair OPTIONAL,
  ...
}

ForwardCertificationPath ::= SEQUENCE OF CrossCertificates

CrossCertificates ::= SET OF Certificate

PkiPath ::= SEQUENCE OF Certificate

-- certificate revocation list (CRL)
CertificateList ::=
  SIGNED{CertificateListContent}

CertificateListContent ::= SEQUENCE {
  version              Version OPTIONAL,
  -- if present, version shall be v2
  signature            AlgorithmIdentifier{{SupportedAlgorithms}},
  issuer               Name,
  thisUpdate           Time,
  nextUpdate           Time OPTIONAL,
  revokedCertificates
    SEQUENCE OF
      SEQUENCE {serialNumber        CertificateSerialNumber,
                revocationDate      Time,
                crlEntryExtensions  Extensions OPTIONAL,
                ...} OPTIONAL,
   ...,
   ...,
  crlExtensions        [0]  Extensions OPTIONAL
}

-- PKI object classes
pkiUser OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {userCertificate}
  ID           id-oc-pkiUser
}

pkiCA OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN
    {cACertificate | certificateRevocationList | authorityRevocationList |
      crossCertificatePair}
  ID           id-oc-pkiCA
}

cRLDistributionPoint OBJECT-CLASS ::= {
  SUBCLASS OF   {top}
  KIND          structural
  MUST CONTAIN  {commonName}
  MAY CONTAIN
    {certificateRevocationList | authorityRevocationList | deltaRevocationList}
  ID            id-oc-cRLDistributionPoint
}

cRLDistPtNameForm NAME-FORM ::= {
  NAMES            cRLDistributionPoint
  WITH ATTRIBUTES  {commonName}
```

```
  ID               id-nf-cRLDistPtNameForm
}

deltaCRL OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {deltaRevocationList}
  ID           id-oc-deltaCRL
}

cpCps OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {certificatePolicy | certificationPracticeStmt}
  ID           id-oc-cpCps
}

pkiCertPath OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {pkiPath}
  ID           id-oc-pkiCertPath
}

-- PKI directory attributes
userCertificate ATTRIBUTE ::= {
  WITH SYNTAX             Certificate
  EQUALITY MATCHING RULE  certificateExactMatch
  ID                      id-at-userCertificate
}

cACertificate ATTRIBUTE ::= {
  WITH SYNTAX             Certificate
  EQUALITY MATCHING RULE  certificateExactMatch
  ID                      id-at-cAcertificate
}

crossCertificatePair ATTRIBUTE ::= {
  WITH SYNTAX             CertificatePair
  EQUALITY MATCHING RULE  certificatePairExactMatch
  ID                      id-at-crossCertificatePair
}

CertificatePair ::= SEQUENCE {
  forward  [0]  Certificate OPTIONAL,
  reverse  [1]  Certificate OPTIONAL,
  -- at least one of the pair shall be present
  ...
}
(WITH COMPONENTS {
   ...,
   forward  PRESENT
 } | WITH COMPONENTS {
       ...,
       reverse  PRESENT
     })

certificateRevocationList ATTRIBUTE ::= {
  WITH SYNTAX             CertificateList
  EQUALITY MATCHING RULE  certificateListExactMatch
  ID                      id-at-certificateRevocationList
}

authorityRevocationList ATTRIBUTE ::= {
  WITH SYNTAX             CertificateList
  EQUALITY MATCHING RULE  certificateListExactMatch
  ID                      id-at-authorityRevocationList
}
```

```
deltaRevocationList ATTRIBUTE ::= {
  WITH SYNTAX             CertificateList
  EQUALITY MATCHING RULE  certificateListExactMatch
  ID                      id-at-deltaRevocationList
}

supportedAlgorithms ATTRIBUTE ::= {
  WITH SYNTAX             SupportedAlgorithm
  EQUALITY MATCHING RULE  algorithmIdentifierMatch
  ID                      id-at-supportedAlgorithms
}

SupportedAlgorithm ::= SEQUENCE {
  algorithmIdentifier          AlgorithmIdentifier{{SupportedAlgorithms}},
  intendedUsage                [0]  KeyUsage OPTIONAL,
  intendedCertificatePolicies  [1]  CertificatePoliciesSyntax OPTIONAL,
  ...
}

certificationPracticeStmt ATTRIBUTE ::= {
  WITH SYNTAX  InfoSyntax
  ID           id-at-certificationPracticeStmt
}

InfoSyntax ::= CHOICE {
  content  UnboundedDirectoryString,
  pointer  SEQUENCE {name  GeneralNames,
                     hash  HASH{HashedPolicyInfo} OPTIONAL,
                     ...},
  ...
}

POLICY ::= TYPE-IDENTIFIER

HashedPolicyInfo ::= POLICY.&Type({Policies})

Policies POLICY ::=
  {...} -- Defined by implementors

certificatePolicy ATTRIBUTE ::= {
  WITH SYNTAX  PolicySyntax
  ID           id-at-certificatePolicy
}

PolicySyntax ::= SEQUENCE {
  policyIdentifier  PolicyID,
  policySyntax      InfoSyntax,
  ...
}

PolicyID ::= CertPolicyId

pkiPath ATTRIBUTE ::= {WITH SYNTAX  PkiPath
                       ID           id-at-pkiPath
}

userPassword ATTRIBUTE ::= {
  WITH SYNTAX             OCTET STRING(SIZE (0..MAX))
  EQUALITY MATCHING RULE  octetStringMatch
  ID                      id-at-userPassword
}

-- object identifier assignments
-- object classes
id-oc-cRLDistributionPoint OBJECT IDENTIFIER ::=
  {id-oc 19}
```

```
id-oc-pkiUser OBJECT IDENTIFIER ::= {id-oc 21}

id-oc-pkiCA OBJECT IDENTIFIER ::= {id-oc 22}

id-oc-deltaCRL OBJECT IDENTIFIER ::= {id-oc 23}

id-oc-cpCps OBJECT IDENTIFIER ::= {id-oc 30}

id-oc-pkiCertPath OBJECT IDENTIFIER ::= {id-oc 31}

-- name forms
id-nf-cRLDistPtNameForm OBJECT IDENTIFIER ::= {id-nf 14}

-- directory attributes
id-at-userPassword OBJECT IDENTIFIER ::= {id-at 35}

id-at-userCertificate OBJECT IDENTIFIER ::= {id-at 36}

id-at-cAcertificate OBJECT IDENTIFIER ::= {id-at 37}

id-at-authorityRevocationList OBJECT IDENTIFIER ::= {id-at 38}

id-at-certificateRevocationList OBJECT IDENTIFIER ::= {id-at 39}

id-at-crossCertificatePair OBJECT IDENTIFIER ::= {id-at 40}

id-at-supportedAlgorithms OBJECT IDENTIFIER ::= {id-at 52}

id-at-deltaRevocationList OBJECT IDENTIFIER ::= {id-at 53}

id-at-certificationPracticeStmt OBJECT IDENTIFIER ::= {id-at 68}

id-at-certificatePolicy OBJECT IDENTIFIER ::= {id-at 69}

id-at-pkiPath OBJECT IDENTIFIER ::= {id-at 70}

END -- AuthenticationFramework


CertificateExtensions {joint-iso-itu-t ds(5) module(1)
  certificateExtensions(26) 6} DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL
IMPORTS
  id-at, id-ce, id-mr, informationFramework, authenticationFramework,
    selectedAttributeTypes
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Name, RelativeDistinguishedName, ATTRIBUTE, Attribute{}, MATCHING-RULE,
    SupportedAttributes
    FROM InformationFramework informationFramework
  CertificateSerialNumber, CertificateList, AlgorithmIdentifier{}, EXTENSION,
    Time, PolicyID, SupportedAlgorithms
    FROM AuthenticationFramework authenticationFramework
  UnboundedDirectoryString
    FROM SelectedAttributeTypes selectedAttributeTypes
  ORAddress
    FROM MTSAbstractService {joint-iso-itu-t mhs(6) mts(3) modules(0)
      mts-abstract-service(1) version-1999(1)};

-- Unless explicitly noted otherwise, there is no significance to the ordering
-- of components of a SEQUENCE OF construct in this Specification.
-- public-key certificate and CRL extensions
authorityKeyIdentifier EXTENSION ::= {
  SYNTAX         AuthorityKeyIdentifier
  IDENTIFIED BY  id-ce-authorityKeyIdentifier
}
```

```
AuthorityKeyIdentifier ::= SEQUENCE {
  keyIdentifier              [0]  KeyIdentifier OPTIONAL,
  authorityCertIssuer        [1]  GeneralNames OPTIONAL,
  authorityCertSerialNumber  [2]  CertificateSerialNumber OPTIONAL,
  ...
}
(WITH COMPONENTS {
   ...,
   authorityCertIssuer        PRESENT,
   authorityCertSerialNumber  PRESENT
 } |
 WITH COMPONENTS {
   ...,
   authorityCertIssuer        ABSENT,
   authorityCertSerialNumber  ABSENT
 })

KeyIdentifier ::= OCTET STRING

subjectKeyIdentifier EXTENSION ::= {
  SYNTAX         SubjectKeyIdentifier
  IDENTIFIED BY  id-ce-subjectKeyIdentifier
}

SubjectKeyIdentifier ::= KeyIdentifier

keyUsage EXTENSION ::= {SYNTAX         KeyUsage
                        IDENTIFIED BY  id-ce-keyUsage
}

KeyUsage ::= BIT STRING {
  digitalSignature(0), contentCommitment(1), keyEncipherment(2),
  dataEncipherment(3), keyAgreement(4), keyCertSign(5), cRLSign(6),
  encipherOnly(7), decipherOnly(8)}

extKeyUsage EXTENSION ::= {
  SYNTAX         SEQUENCE SIZE (1..MAX) OF KeyPurposeId
  IDENTIFIED BY  id-ce-extKeyUsage
}

KeyPurposeId ::= OBJECT IDENTIFIER

privateKeyUsagePeriod EXTENSION ::= {
  SYNTAX         PrivateKeyUsagePeriod
  IDENTIFIED BY  id-ce-privateKeyUsagePeriod
}

PrivateKeyUsagePeriod ::= SEQUENCE {
  notBefore  [0]  GeneralizedTime OPTIONAL,
  notAfter   [1]  GeneralizedTime OPTIONAL,
  ...
}
(WITH COMPONENTS {
   ...,
   notBefore  PRESENT
 } | WITH COMPONENTS {
       ...,
       notAfter  PRESENT
     })

certificatePolicies EXTENSION ::= {
  SYNTAX         CertificatePoliciesSyntax
  IDENTIFIED BY  id-ce-certificatePolicies
}

CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation
```

```
PolicyInformation ::= SEQUENCE {
  policyIdentifier  CertPolicyId,
  policyQualifiers  SEQUENCE SIZE (1..MAX) OF PolicyQualifierInfo OPTIONAL,
  ...
}

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
  policyQualifierId  CERT-POLICY-QUALIFIER.&id({SupportedPolicyQualifiers}),
  qualifier
    CERT-POLICY-QUALIFIER.&Qualifier
      ({SupportedPolicyQualifiers}{@policyQualifierId}) OPTIONAL,
  ...
}

SupportedPolicyQualifiers CERT-POLICY-QUALIFIER ::=
  {...}

anyPolicy OBJECT IDENTIFIER ::= {2 5 29 32 0}

CERT-POLICY-QUALIFIER ::= CLASS {
  &id         OBJECT IDENTIFIER UNIQUE,
  &Qualifier  OPTIONAL
}WITH SYNTAX {POLICY-QUALIFIER-ID &id
              [QUALIFIER-TYPE &Qualifier]
}

policyMappings EXTENSION ::= {
  SYNTAX         PolicyMappingsSyntax
  IDENTIFIED BY  id-ce-policyMappings
}

PolicyMappingsSyntax ::=
  SEQUENCE SIZE (1..MAX) OF
    SEQUENCE {issuerDomainPolicy   CertPolicyId,
              subjectDomainPolicy  CertPolicyId,
              ...}

subjectAltName EXTENSION ::= {
  SYNTAX         GeneralNames
  IDENTIFIED BY  id-ce-subjectAltName
}

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
  otherName                 [0]  INSTANCE OF OTHER-NAME,
  rfc822Name                [1]  IA5String,
  dNSName                   [2]  IA5String,
  x400Address               [3]  ORAddress,
  directoryName             [4]  Name,
  ediPartyName              [5]  EDIPartyName,
  uniformResourceIdentifier [6]  IA5String,
  iPAddress                 [7]  OCTET STRING,
  registeredID              [8]  OBJECT IDENTIFIER,
  ...
}

OTHER-NAME ::= TYPE-IDENTIFIER

EDIPartyName ::= SEQUENCE {
  nameAssigner  [0]  UnboundedDirectoryString OPTIONAL,
  partyName     [1]  UnboundedDirectoryString,
  ...
}

issuerAltName EXTENSION ::= {
```

```
  SYNTAX         GeneralNames
  IDENTIFIED BY  id-ce-issuerAltName
}

subjectDirectoryAttributes EXTENSION ::= {
  SYNTAX         AttributesSyntax
  IDENTIFIED BY  id-ce-subjectDirectoryAttributes
}

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}}

basicConstraints EXTENSION ::= {
  SYNTAX         BasicConstraintsSyntax
  IDENTIFIED BY  id-ce-basicConstraints
}

BasicConstraintsSyntax ::= SEQUENCE {
  cA                 BOOLEAN DEFAULT FALSE,
  pathLenConstraint  INTEGER(0..MAX) OPTIONAL,
  ...
}

nameConstraints EXTENSION ::= {
  SYNTAX         NameConstraintsSyntax
  IDENTIFIED BY  id-ce-nameConstraints
}

NameConstraintsSyntax ::= SEQUENCE {
  permittedSubtrees  [0]  GeneralSubtrees OPTIONAL,
  excludedSubtrees   [1]  GeneralSubtrees OPTIONAL,
  ...
}(ALL EXCEPT ({ -- none; at least one component shall be present --}))

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
  base     GeneralName,
  minimum  [0]  BaseDistance DEFAULT 0,
  maximum  [1]  BaseDistance OPTIONAL,
  ...
}

BaseDistance ::= INTEGER(0..MAX)

policyConstraints EXTENSION ::= {
  SYNTAX         PolicyConstraintsSyntax
  IDENTIFIED BY  id-ce-policyConstraints
}

PolicyConstraintsSyntax ::= SEQUENCE {
  requireExplicitPolicy  [0]  SkipCerts OPTIONAL,
  inhibitPolicyMapping   [1]  SkipCerts OPTIONAL,
  ...
}

SkipCerts ::= INTEGER(0..MAX)

inhibitAnyPolicy EXTENSION ::= {
  SYNTAX         SkipCerts
  IDENTIFIED BY  id-ce-inhibitAnyPolicy
}

cRLNumber EXTENSION ::= {
  SYNTAX         CRLNumber
  IDENTIFIED BY  id-ce-cRLNumber
}

CRLNumber ::= INTEGER(0..MAX)
```

```
reasonCode EXTENSION ::= {
  SYNTAX         CRLReason
  IDENTIFIED BY  id-ce-reasonCode
}

CRLReason ::= ENUMERATED {
  unspecified(0), keyCompromise(1), cACompromise(2), affiliationChanged(3),
  superseded(4), cessationOfOperation(5), certificateHold(6), removeFromCRL(8),
  privilegeWithdrawn(9), aaCompromise(10),...}

holdInstructionCode EXTENSION ::= {
  SYNTAX         HoldInstruction
  IDENTIFIED BY  id-ce-instructionCode
}

HoldInstruction ::= OBJECT IDENTIFIER

invalidityDate EXTENSION ::= {
  SYNTAX         GeneralizedTime
  IDENTIFIED BY  id-ce-invalidityDate
}

crlScope EXTENSION ::= {
  SYNTAX         CRLScopeSyntax
  IDENTIFIED BY  id-ce-cRLScope
}

CRLScopeSyntax ::= SEQUENCE SIZE (1..MAX) OF PerAuthorityScope

PerAuthorityScope ::= SEQUENCE {
  authorityName       [0]  GeneralName OPTIONAL,
  distributionPoint   [1]  DistributionPointName OPTIONAL,
  onlyContains        [2]  OnlyCertificateTypes OPTIONAL,
  onlySomeReasons     [4]  ReasonFlags OPTIONAL,
  serialNumberRange   [5]  NumberRange OPTIONAL,
  subjectKeyIdRange   [6]  NumberRange OPTIONAL,
  nameSubtrees        [7]  GeneralNames OPTIONAL,
  baseRevocationInfo  [9]  BaseRevocationInfo OPTIONAL,
  ...
}

OnlyCertificateTypes ::= BIT STRING {user(0), authority(1), attribute(2)}

NumberRange ::= SEQUENCE {
  startingNumber  [0]  INTEGER OPTIONAL,
  endingNumber    [1]  INTEGER OPTIONAL,
  modulus         INTEGER OPTIONAL,
  ...
}

BaseRevocationInfo ::= SEQUENCE {
  cRLStreamIdentifier  [0]  CRLStreamIdentifier OPTIONAL,
  cRLNumber            [1]  CRLNumber,
  baseThisUpdate       [2]  GeneralizedTime,
  ...
}

statusReferrals EXTENSION ::= {
  SYNTAX         StatusReferrals
  IDENTIFIED BY  id-ce-statusReferrals
}

StatusReferrals ::= SEQUENCE SIZE (1..MAX) OF StatusReferral

StatusReferral ::= CHOICE {
  cRLReferral    [0]  CRLReferral,
  otherReferral  [1]  INSTANCE OF OTHER-REFERRAL,
```

```
  ...
}

CRLReferral ::= SEQUENCE {
  issuer          [0]  GeneralName OPTIONAL,
  location        [1]  GeneralName OPTIONAL,
  deltaRefInfo    [2]  DeltaRefInfo OPTIONAL,
  cRLScope        CRLScopeSyntax,
  lastUpdate      [3]  GeneralizedTime OPTIONAL,
  lastChangedCRL  [4]  GeneralizedTime OPTIONAL,
  ...
}

DeltaRefInfo ::= SEQUENCE {
  deltaLocation  GeneralName,
  lastDelta      GeneralizedTime OPTIONAL,
  ...
}

OTHER-REFERRAL ::= TYPE-IDENTIFIER

cRLStreamIdentifier EXTENSION ::= {
  SYNTAX         CRLStreamIdentifier
  IDENTIFIED BY  id-ce-cRLStreamIdentifier
}

CRLStreamIdentifier ::= INTEGER(0..MAX)

orderedList EXTENSION ::= {
  SYNTAX         OrderedListSyntax
  IDENTIFIED BY  id-ce-orderedList
}

OrderedListSyntax ::= ENUMERATED {ascSerialNum(0), ascRevDate(1),...}

deltaInfo EXTENSION ::= {
  SYNTAX         DeltaInformation
  IDENTIFIED BY  id-ce-deltaInfo
}

DeltaInformation ::= SEQUENCE {
  deltaLocation  GeneralName,
  nextDelta      GeneralizedTime OPTIONAL,
  ...
}

toBeRevoked EXTENSION ::= {
  SYNTAX         ToBeRevokedSyntax
  IDENTIFIED BY  id-ce-toBeRevoked
}

ToBeRevokedSyntax ::= SEQUENCE SIZE (1..MAX) OF ToBeRevokedGroup

ToBeRevokedGroup ::= SEQUENCE {
  certificateIssuer  [0]  GeneralName OPTIONAL,
  reasonInfo         [1]  ReasonInfo OPTIONAL,
  revocationTime     GeneralizedTime,
  certificateGroup   CertificateGroup,
  ...
}

ReasonInfo ::= SEQUENCE {
  reasonCode           CRLReason,
  holdInstructionCode  HoldInstruction OPTIONAL,
  ...
}

CertificateGroup ::= CHOICE {
```

```
  serialNumbers      [0]  CertificateSerialNumbers,
  serialNumberRange  [1]  CertificateGroupNumberRange,
  nameSubtree        [2]  GeneralName,
  ...
}

CertificateGroupNumberRange ::= SEQUENCE {
  startingNumber  [0]  INTEGER,
  endingNumber    [1]  INTEGER,
  ...
}

CertificateSerialNumbers ::= SEQUENCE SIZE (1..MAX) OF CertificateSerialNumber

revokedGroups EXTENSION ::= {
  SYNTAX         RevokedGroupsSyntax
  IDENTIFIED BY  id-ce-RevokedGroups
}

RevokedGroupsSyntax ::= SEQUENCE SIZE (1..MAX) OF RevokedGroup

RevokedGroup ::= SEQUENCE {
  certificateIssuer        [0]  GeneralName OPTIONAL,
  reasonInfo               [1]  ReasonInfo OPTIONAL,
  invalidityDate           [2]  GeneralizedTime OPTIONAL,
  revokedcertificateGroup  [3]  RevokedCertificateGroup,
  ...
}

RevokedCertificateGroup ::= CHOICE {
  serialNumberRange  NumberRange,
  nameSubtree        GeneralName
}

expiredCertsOnCRL EXTENSION ::= {
  SYNTAX         ExpiredCertsOnCRL
  IDENTIFIED BY  id-ce-expiredCertsOnCRL
}

ExpiredCertsOnCRL ::= GeneralizedTime

cRLDistributionPoints EXTENSION ::= {
  SYNTAX         CRLDistPointsSyntax
  IDENTIFIED BY  id-ce-cRLDistributionPoints
}

CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
  distributionPoint  [0]  DistributionPointName OPTIONAL,
  reasons            [1]  ReasonFlags OPTIONAL,
  cRLIssuer          [2]  GeneralNames OPTIONAL,
  ...
}

DistributionPointName ::= CHOICE {
  fullName                 [0]  GeneralNames,
  nameRelativeToCRLIssuer  [1]  RelativeDistinguishedName,
  ...
}

ReasonFlags ::= BIT STRING {
  unused(0), keyCompromise(1), cACompromise(2), affiliationChanged(3),
  superseded(4), cessationOfOperation(5), certificateHold(6),
  privilegeWithdrawn(7), aACompromise(8)}

issuingDistributionPoint EXTENSION ::= {
  SYNTAX         IssuingDistPointSyntax
```

```
  IDENTIFIED BY  id-ce-issuingDistributionPoint
}

IssuingDistPointSyntax ::= SEQUENCE {
  -- If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE,
  -- the CRL covers both certificate types
  distributionPoint               [0]  DistributionPointName OPTIONAL,
  onlyContainsUserPublicKeyCerts  [1]  BOOLEAN DEFAULT FALSE,
  onlyContainsCACerts             [2]  BOOLEAN DEFAULT FALSE,
  onlySomeReasons                 [3]  ReasonFlags OPTIONAL,
  indirectCRL                     [4]  BOOLEAN DEFAULT FALSE,
  ...
}

certificateIssuer EXTENSION ::= {
  SYNTAX         GeneralNames
  IDENTIFIED BY  id-ce-certificateIssuer
}

deltaCRLIndicator EXTENSION ::= {
  SYNTAX         BaseCRLNumber
  IDENTIFIED BY  id-ce-deltaCRLIndicator
}

BaseCRLNumber ::= CRLNumber

baseUpdateTime EXTENSION ::= {
  SYNTAX         GeneralizedTime
  IDENTIFIED BY  id-ce-baseUpdateTime
}

freshestCRL EXTENSION ::= {
  SYNTAX         CRLDistPointsSyntax
  IDENTIFIED BY  id-ce-freshestCRL
}

aAissuingDistributionPoint EXTENSION ::= {
  SYNTAX         AAIssuingDistPointSyntax
  IDENTIFIED BY  id-ce-aAissuingDistributionPoint
}

AAIssuingDistPointSyntax ::= SEQUENCE {
  distributionPoint           [0]  DistributionPointName OPTIONAL,
  onlySomeReasons             [1]  ReasonFlags OPTIONAL,
  indirectCRL                 [2]  BOOLEAN DEFAULT FALSE,
  containsUserAttributeCerts  [3]  BOOLEAN DEFAULT TRUE,
  containsAACerts             [4]  BOOLEAN DEFAULT TRUE,
  containsSOAPublicKeyCerts   [5]  BOOLEAN DEFAULT TRUE,
  ...
}

-- PKI matching rules
certificateExactMatch MATCHING-RULE ::= {
  SYNTAX  CertificateExactAssertion
  ID      id-mr-certificateExactMatch
}

CertificateExactAssertion ::= SEQUENCE {
  serialNumber  CertificateSerialNumber,
  issuer        Name,
  ...
}

certificateMatch MATCHING-RULE ::= {
  SYNTAX  CertificateAssertion
  ID      id-mr-certificateMatch
}
```

```
CertificateAssertion ::= SEQUENCE {
  serialNumber            [0]  CertificateSerialNumber OPTIONAL,
  issuer                  [1]  Name OPTIONAL,
  subjectKeyIdentifier    [2]  SubjectKeyIdentifier OPTIONAL,
  authorityKeyIdentifier  [3]  AuthorityKeyIdentifier OPTIONAL,
  certificateValid        [4]  Time OPTIONAL,
  privateKeyValid         [5]  GeneralizedTime OPTIONAL,
  subjectPublicKeyAlgID   [6]  OBJECT IDENTIFIER OPTIONAL,
  keyUsage                [7]  KeyUsage OPTIONAL,
  subjectAltName          [8]  AltNameType OPTIONAL,
  policy                  [9]  CertPolicySet OPTIONAL,
  pathToName              [10]  Name OPTIONAL,
  subject                 [11]  Name OPTIONAL,
  nameConstraints         [12]  NameConstraintsSyntax OPTIONAL,
  ...
}

AltNameType ::= CHOICE {
  builtinNameForm
    ENUMERATED {rfc822Name(1), dNSName(2), x400Address(3), directoryName(4),
                ediPartyName(5), uniformResourceIdentifier(6), iPAddress(7),
                registeredId(8),...},
  otherNameForm    OBJECT IDENTIFIER,
  ...
}

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

certificatePairExactMatch MATCHING-RULE ::= {
  SYNTAX  CertificatePairExactAssertion
  ID      id-mr-certificatePairExactMatch
}

CertificatePairExactAssertion ::= SEQUENCE {
  issuedToThisCAAssertion  [0]  CertificateExactAssertion OPTIONAL,
  issuedByThisCAAssertion  [1]  CertificateExactAssertion OPTIONAL,
  ...
}
(WITH COMPONENTS {
   ...,
   issuedToThisCAAssertion  PRESENT
 } | WITH COMPONENTS {
       ...,
       issuedByThisCAAssertion  PRESENT
     })

certificatePairMatch MATCHING-RULE ::= {
  SYNTAX  CertificatePairAssertion
  ID      id-mr-certificatePairMatch
}

CertificatePairAssertion ::= SEQUENCE {
  issuedToThisCAAssertion  [0]  CertificateAssertion OPTIONAL,
  issuedByThisCAAssertion  [1]  CertificateAssertion OPTIONAL,
  ...
}
(WITH COMPONENTS {
   ...,
   issuedToThisCAAssertion  PRESENT
 } | WITH COMPONENTS {
       ...,
       issuedByThisCAAssertion  PRESENT
     })

certificateListExactMatch MATCHING-RULE ::= {
  SYNTAX  CertificateListExactAssertion
  ID      id-mr-certificateListExactMatch
}
```

```
CertificateListExactAssertion ::= SEQUENCE {
  issuer             Name,
  thisUpdate         Time,
  distributionPoint  DistributionPointName OPTIONAL
}

certificateListMatch MATCHING-RULE ::= {
  SYNTAX  CertificateListAssertion
  ID      id-mr-certificateListMatch
}

CertificateListAssertion ::= SEQUENCE {
  issuer                  Name OPTIONAL,
  minCRLNumber            [0]  CRLNumber OPTIONAL,
  maxCRLNumber            [1]  CRLNumber OPTIONAL,
  reasonFlags             ReasonFlags OPTIONAL,
  dateAndTime             Time OPTIONAL,
  distributionPoint       [2]  DistributionPointName OPTIONAL,
  authorityKeyIdentifier  [3]  AuthorityKeyIdentifier OPTIONAL,
  ...
}

algorithmIdentifierMatch MATCHING-RULE ::= {
  SYNTAX  AlgorithmIdentifier {{SupportedAlgorithms}}
  ID      id-mr-algorithmIdentifierMatch
}

policyMatch MATCHING-RULE ::= {SYNTAX  PolicyID
                               ID      id-mr-policyMatch
}

pkiPathMatch MATCHING-RULE ::= {
  SYNTAX  PkiPathMatchSyntax
  ID      id-mr-pkiPathMatch
}

PkiPathMatchSyntax ::= SEQUENCE {firstIssuer  Name,
                                 lastSubject  Name,
                                 ...
}

enhancedCertificateMatch MATCHING-RULE ::= {
  SYNTAX  EnhancedCertificateAssertion
  ID      id-mr-enhancedCertificateMatch
}

EnhancedCertificateAssertion ::= SEQUENCE {
  serialNumber            [0]  CertificateSerialNumber OPTIONAL,
  issuer                  [1]  Name OPTIONAL,
  subjectKeyIdentifier    [2]  SubjectKeyIdentifier OPTIONAL,
  authorityKeyIdentifier  [3]  AuthorityKeyIdentifier OPTIONAL,
  certificateValid        [4]  Time OPTIONAL,
  privateKeyValid         [5]  GeneralizedTime OPTIONAL,
  subjectPublicKeyAlgID   [6]  OBJECT IDENTIFIER OPTIONAL,
  keyUsage                [7]  KeyUsage OPTIONAL,
  subjectAltName          [8]  AltName OPTIONAL,
  policy                  [9]  CertPolicySet OPTIONAL,
  pathToName              [10]  GeneralNames OPTIONAL,
  subject                 [11]  Name OPTIONAL,
  nameConstraints         [12]  NameConstraintsSyntax OPTIONAL,
  ...
}(ALL EXCEPT ({ -- none; at least one component shall be present --}))

AltName ::= SEQUENCE {
  altnameType   AltNameType,
  altNameValue  GeneralName OPTIONAL
}
```

```
-- Object identifier assignments
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::=
  {id-ce 9}

id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= {id-ce 14}

id-ce-keyUsage OBJECT IDENTIFIER ::= {id-ce 15}

id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::= {id-ce 16}

id-ce-subjectAltName OBJECT IDENTIFIER ::= {id-ce 17}

id-ce-issuerAltName OBJECT IDENTIFIER ::= {id-ce 18}

id-ce-basicConstraints OBJECT IDENTIFIER ::= {id-ce 19}

id-ce-cRLNumber OBJECT IDENTIFIER ::= {id-ce 20}

id-ce-reasonCode OBJECT IDENTIFIER ::= {id-ce 21}

id-ce-instructionCode OBJECT IDENTIFIER ::= {id-ce 23}

id-ce-invalidityDate OBJECT IDENTIFIER ::= {id-ce 24}

id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= {id-ce 27}

id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= {id-ce 28}

id-ce-certificateIssuer OBJECT IDENTIFIER ::= {id-ce 29}

id-ce-nameConstraints OBJECT IDENTIFIER ::= {id-ce 30}

id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= {id-ce 31}

id-ce-certificatePolicies OBJECT IDENTIFIER ::= {id-ce 32}

id-ce-policyMappings OBJECT IDENTIFIER ::= {id-ce 33}

-- deprecated                    OBJECT IDENTIFIER  ::=  {id-ce 34}
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::=
  {id-ce 35}

id-ce-policyConstraints OBJECT IDENTIFIER ::= {id-ce 36}

id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}

id-ce-cRLStreamIdentifier OBJECT IDENTIFIER ::= {id-ce 40}

id-ce-cRLScope OBJECT IDENTIFIER ::= {id-ce 44}

id-ce-statusReferrals OBJECT IDENTIFIER ::= {id-ce 45}

id-ce-freshestCRL OBJECT IDENTIFIER ::= {id-ce 46}

id-ce-orderedList OBJECT IDENTIFIER ::= {id-ce 47}

id-ce-baseUpdateTime OBJECT IDENTIFIER ::= {id-ce 51}

id-ce-deltaInfo OBJECT IDENTIFIER ::= {id-ce 53}

id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= {id-ce 54}

id-ce-toBeRevoked OBJECT IDENTIFIER ::= {id-ce 58}

id-ce-RevokedGroups OBJECT IDENTIFIER ::= {id-ce 59}

id-ce-expiredCertsOnCRL OBJECT IDENTIFIER ::= {id-ce 60}
```

```
id-ce-aAissuingDistributionPoint OBJECT IDENTIFIER ::= {id-ce 63}

-- matching rule OIDs
id-mr-certificateExactMatch OBJECT IDENTIFIER ::=
  {id-mr 34}

id-mr-certificateMatch OBJECT IDENTIFIER ::= {id-mr 35}

id-mr-certificatePairExactMatch OBJECT IDENTIFIER ::= {id-mr 36}

id-mr-certificatePairMatch OBJECT IDENTIFIER ::= {id-mr 37}

id-mr-certificateListExactMatch OBJECT IDENTIFIER ::= {id-mr 38}

id-mr-certificateListMatch OBJECT IDENTIFIER ::= {id-mr 39}

id-mr-algorithmIdentifierMatch OBJECT IDENTIFIER ::= {id-mr 40}

id-mr-policyMatch OBJECT IDENTIFIER ::= {id-mr 60}

id-mr-pkiPathMatch OBJECT IDENTIFIER ::= {id-mr 62}

id-mr-enhancedCertificateMatch OBJECT IDENTIFIER ::= {id-mr 65}

-- The following OBJECT IDENTIFIERS are not used by this Specification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}
END -- CertificateExtensions


AttributeCertificateDefinitions {joint-iso-itu-t ds(5) module(1)
  attributeCertificateDefinitions(32) 6} DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL
IMPORTS
  basicAccessControl, id-at, id-ce, id-mr, informationFramework,
    authenticationFramework, selectedAttributeTypes, id-oc,
    certificateExtensions, externalDefinitions
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  ATTRIBUTE, Attribute{}, AttributeType, MATCHING-RULE, Name, OBJECT-CLASS,
    RelativeDistinguishedName, SupportedAttributes, top
    FROM InformationFramework informationFramework
  AttributeTypeAndValue
    FROM BasicAccessControl basicAccessControl
  AlgorithmIdentifier, Certificate, CertificateList, CertificateSerialNumber,
    EXTENSION, Extensions, InfoSyntax, PolicySyntax, SIGNED{},
    SupportedAlgorithms
    FROM AuthenticationFramework authenticationFramework
  TimeSpecification, UnboundedDirectoryString, UniqueIdentifier
    FROM SelectedAttributeTypes selectedAttributeTypes
  certificateListExactMatch, GeneralName, GeneralNames, NameConstraintsSyntax
    FROM CertificateExtensions certificateExtensions
  UserNotice
    FROM PKIX1Implicit93 {iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-implicit-93(4)};

-- Unless explicitly noted otherwise, there is no significance to the ordering
-- of components of a SEQUENCE OF construct in this Specification.
-- attribute certificate constructs
AttributeCertificate ::=
  SIGNED{AttributeCertificateInfo}

AttributeCertificateInfo ::= SEQUENCE {
  version                AttCertVersion, -- version is v2
```

```
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier{{SupportedAlgorithms}},
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute{{SupportedAttributes}},
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  ...,
  extensions              Extensions OPTIONAL
}

AttCertVersion ::= INTEGER {v2(1)}

Holder ::= SEQUENCE {
  baseCertificateID  [0]  IssuerSerial OPTIONAL,
  -- the issuer and serial number of  the holder's Public Key Certificate
  entityName         [1]  GeneralNames OPTIONAL,
  -- the name of the entity or role
  objectDigestInfo   [2]  ObjectDigestInfo OPTIONAL-- used to directly authenticate the
holder, e.g., an executable
-- at least one of baseCertificateID, entityName or objectDigestInfo shall be present
}

ObjectDigestInfo ::= SEQUENCE {
  digestedObjectType
    ENUMERATED {publicKey(0), publicKeyCert(1), otherObjectTypes(2)},
  otherObjectTypeID   OBJECT IDENTIFIER OPTIONAL,
  digestAlgorithm     AlgorithmIdentifier{{SupportedAlgorithms}},
  objectDigest        BIT STRING,
  ...
}

AttCertIssuer ::= [0]  SEQUENCE {
  issuerName         GeneralNames OPTIONAL,
  baseCertificateID  [0]  IssuerSerial OPTIONAL,
  objectDigestInfo   [1]  ObjectDigestInfo OPTIONAL,
  ...
}
-- At least one component shall be present
(WITH COMPONENTS {
   ...,
   issuerName  PRESENT
 } | WITH COMPONENTS {
       ...,
       baseCertificateID  PRESENT
     } | WITH COMPONENTS {
           ...,
           objectDigestInfo  PRESENT
         })

IssuerSerial ::= SEQUENCE {
  issuer     GeneralNames,
  serial     CertificateSerialNumber,
  issuerUID  UniqueIdentifier OPTIONAL,
  ...
}

AttCertValidityPeriod ::= SEQUENCE {
  notBeforeTime  GeneralizedTime,
  notAfterTime   GeneralizedTime,
  ...
}

AttributeCertificationPath ::= SEQUENCE {
  attributeCertificate  AttributeCertificate,
  acPath                SEQUENCE OF ACPathData OPTIONAL,
  ...
}
```

```
ACPathData ::= SEQUENCE {
  certificate           [0]  Certificate OPTIONAL,
  attributeCertificate  [1]  AttributeCertificate OPTIONAL,
  ...
}

PrivilegePolicy ::= OBJECT IDENTIFIER

-- privilege attributes
role ATTRIBUTE ::= {WITH SYNTAX  RoleSyntax
                    ID           id-at-role
}

RoleSyntax ::= SEQUENCE {
  roleAuthority  [0]  GeneralNames OPTIONAL,
  roleName       [1]  GeneralName,
  ...
}

xmlPrivilegeInfo ATTRIBUTE ::= {
  WITH SYNTAX  UTF8String --contains XML-encoded privilege information
  ID           id-at-xMLPrivilegeInfo
}

permission ATTRIBUTE ::= {
  WITH SYNTAX             DualStringSyntax
  EQUALITY MATCHING RULE  dualStringMatch
  ID                      id-at-permission
}

DualStringSyntax ::= SEQUENCE {
  operation  [0]  UnboundedDirectoryString,
  object     [1]  UnboundedDirectoryString,
  ...
}

dualStringMatch MATCHING-RULE ::= {
  SYNTAX  DualStringSyntax
  ID      id-mr-dualStringMatch
}

timeSpecification EXTENSION ::= {
  SYNTAX         TimeSpecification
  IDENTIFIED BY  id-ce-timeSpecification
}

timeSpecificationMatch MATCHING-RULE ::= {
  SYNTAX  TimeSpecification
  ID      id-mr-timeSpecMatch
}

targetingInformation EXTENSION ::= {
  SYNTAX         SEQUENCE SIZE (1..MAX) OF Targets
  IDENTIFIED BY  id-ce-targetInformation
}

Targets ::= SEQUENCE SIZE (1..MAX) OF Target

Target ::= CHOICE {
  targetName   [0]  GeneralName,
  targetGroup  [1]  GeneralName,
  targetCert   [2]  TargetCert,
  ...
}

TargetCert ::= SEQUENCE {
  targetCertificate  IssuerSerial,
```

```
  targetName         GeneralName OPTIONAL,
  certDigestInfo     ObjectDigestInfo OPTIONAL
}

userNotice EXTENSION ::= {
  SYNTAX         SEQUENCE SIZE (1..MAX) OF UserNotice
  IDENTIFIED BY  id-ce-userNotice
}

acceptablePrivilegePolicies EXTENSION ::= {
  SYNTAX         AcceptablePrivilegePoliciesSyntax
  IDENTIFIED BY  id-ce-acceptablePrivilegePolicies
}

AcceptablePrivilegePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PrivilegePolicy

singleUse EXTENSION ::= {SYNTAX         NULL
                         IDENTIFIED BY  id-ce-singleUse
}

groupAC EXTENSION ::= {SYNTAX         NULL
                       IDENTIFIED BY  id-ce-groupAC
}

noRevAvail EXTENSION ::= {SYNTAX         NULL
                          IDENTIFIED BY  id-ce-noRevAvail
}

sOAIdentifier EXTENSION ::= {
  SYNTAX         NULL
  IDENTIFIED BY  id-ce-sOAIdentifier
}

sOAIdentifierMatch MATCHING-RULE ::= {
  SYNTAX  NULL
  ID      id-mr-sOAIdentifierMatch
}

attributeDescriptor EXTENSION ::= {
  SYNTAX         AttributeDescriptorSyntax
  IDENTIFIED BY  {id-ce-attributeDescriptor}
}

AttributeDescriptorSyntax ::= SEQUENCE {
  identifier       AttributeIdentifier,
  attributeSyntax  OCTET STRING(SIZE (1..MAX)),
  name             [0]  AttributeName OPTIONAL,
  description      [1]  AttributeDescription OPTIONAL,
  dominationRule   PrivilegePolicyIdentifier,
  ...
}

AttributeIdentifier ::= ATTRIBUTE.&id({AttributeIDs})

AttributeIDs ATTRIBUTE ::=
  {...}

AttributeName ::= UTF8String(SIZE (1..MAX))

AttributeDescription ::= UTF8String(SIZE (1..MAX))

PrivilegePolicyIdentifier ::= SEQUENCE {
  privilegePolicy  PrivilegePolicy,
  privPolSyntax    InfoSyntax,
  ...
}

attDescriptor MATCHING-RULE ::= {
```

```
  SYNTAX  AttributeDescriptorSyntax
  ID      id-mr-attDescriptorMatch
}

roleSpecCertIdentifier EXTENSION ::= {
  SYNTAX         RoleSpecCertIdentifierSyntax
  IDENTIFIED BY  {id-ce-roleSpecCertIdentifier}
}

RoleSpecCertIdentifierSyntax ::=
  SEQUENCE SIZE (1..MAX) OF RoleSpecCertIdentifier

RoleSpecCertIdentifier ::= SEQUENCE {
  roleName              [0]  GeneralName,
  roleCertIssuer        [1]  GeneralName,
  roleCertSerialNumber  [2]  CertificateSerialNumber OPTIONAL,
  roleCertLocator       [3]  GeneralNames OPTIONAL,
  ...
}

roleSpecCertIdMatch MATCHING-RULE ::= {
  SYNTAX  RoleSpecCertIdentifierSyntax
  ID      id-mr-roleSpecCertIdMatch
}

basicAttConstraints EXTENSION ::= {
  SYNTAX         BasicAttConstraintsSyntax
  IDENTIFIED BY  {id-ce-basicAttConstraints}
}

BasicAttConstraintsSyntax ::= SEQUENCE {
  authority          BOOLEAN DEFAULT FALSE,
  pathLenConstraint  INTEGER(0..MAX) OPTIONAL,
  ...
}

basicAttConstraintsMatch MATCHING-RULE ::= {
  SYNTAX  BasicAttConstraintsSyntax
  ID      id-mr-basicAttConstraintsMatch
}

delegatedNameConstraints EXTENSION ::= {
  SYNTAX         NameConstraintsSyntax
  IDENTIFIED BY  id-ce-delegatedNameConstraints
}

delegatedNameConstraintsMatch MATCHING-RULE ::= {
  SYNTAX  NameConstraintsSyntax
  ID      id-mr-delegatedNameConstraintsMatch
}

acceptableCertPolicies EXTENSION ::= {
  SYNTAX         AcceptableCertPoliciesSyntax
  IDENTIFIED BY  id-ce-acceptableCertPolicies
}

AcceptableCertPoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

CertPolicyId ::= OBJECT IDENTIFIER

acceptableCertPoliciesMatch MATCHING-RULE ::= {
  SYNTAX  AcceptableCertPoliciesSyntax
  ID      id-mr-acceptableCertPoliciesMatch
}

authorityAttributeIdentifier EXTENSION ::= {
  SYNTAX         AuthorityAttributeIdentifierSyntax
  IDENTIFIED BY  {id-ce-authorityAttributeIdentifier}
```

```
}

AuthorityAttributeIdentifierSyntax ::= SEQUENCE SIZE (1..MAX) OF AuthAttId

AuthAttId ::= IssuerSerial

authAttIdMatch MATCHING-RULE ::= {
  SYNTAX  AuthorityAttributeIdentifierSyntax
  ID      id-mr-authAttIdMatch
}

indirectIssuer EXTENSION ::= {
  SYNTAX         NULL
  IDENTIFIED BY  id-ce-indirectIssuer
}

issuedOnBehalfOf EXTENSION ::= {
  SYNTAX         GeneralName
  IDENTIFIED BY  id-ce-issuedOnBehalfOf
}

noAssertion EXTENSION ::= {SYNTAX         NULL
                           IDENTIFIED BY  id-ce-noAssertion
}

allowedAttributeAssignments EXTENSION ::= {
  SYNTAX         AllowedAttributeAssignments
  IDENTIFIED BY  id-ce-allowedAttAss
}

AllowedAttributeAssignments ::=
  SET OF
    SEQUENCE {attributes
                [0]  SET OF
                       CHOICE {attributeType           [0]  AttributeType,
                               attributeTypeandValues
                                 [1]  Attribute{{SupportedAttributes}},
                               ...
                       },
              holderDomain  [1]  GeneralName,
              ...
  }

attributeMappings EXTENSION ::= {
  SYNTAX         AttributeMappings
  IDENTIFIED BY  id-ce-attributeMappings
}

AttributeMappings ::=
  SET OF
    CHOICE {typeMappings
              [0]  SEQUENCE {local   [0]  AttributeType,
                             remote  [1]  AttributeType},
            typeValueMappings
              [1]  SEQUENCE {local   [0]  AttributeTypeAndValue,
                             remote  [1]  AttributeTypeAndValue,
            ...}}

holderNameConstraints EXTENSION ::= {
  SYNTAX         HolderNameConstraintsSyntax
  IDENTIFIED BY  id-ce-holderNameConstraints
}

HolderNameConstraintsSyntax ::= SEQUENCE {
  permittedSubtrees  [0]  GeneralSubtrees,
  excludedSubtrees   [1]  GeneralSubtrees OPTIONAL,
  ...
}
```

```
GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
  base     GeneralName,
  minimum  [0]  BaseDistance DEFAULT 0,
  maximum  [1]  BaseDistance OPTIONAL,
  ...
}

BaseDistance ::= INTEGER(0..MAX)

-- PMI object classes
pmiUser OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {attributeCertificateAttribute}
  ID           id-oc-pmiUser
}

pmiAA OBJECT-CLASS ::= { -- a PMI AA
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN
    {aACertificate | attributeCertificateRevocationList |
      attributeAuthorityRevocationList}
  ID           id-oc-pmiAA
}

pmiSOA OBJECT-CLASS ::= { -- a PMI Source of Authority
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN
    {attributeCertificateRevocationList | attributeAuthorityRevocationList |
      attributeDescriptorCertificate}
  ID           id-oc-pmiSOA
}

attCertCRLDistributionPt OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN
    {attributeCertificateRevocationList | attributeAuthorityRevocationList}
  ID           id-oc-attCertCRLDistributionPts
}

pmiDelegationPath OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {delegationPath}
  ID           id-oc-pmiDelegationPath
}

privilegePolicy OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {privPolicy}
  ID           id-oc-privilegePolicy
}

protectedPrivilegePolicy OBJECT-CLASS ::= {
  SUBCLASS OF  {top}
  KIND         auxiliary
  MAY CONTAIN  {protPrivPolicy}
  ID           id-oc-protectedPrivilegePolicy
}

-- PMI directory attributes
```

```
attributeCertificateAttribute ATTRIBUTE ::= {
  WITH SYNTAX             AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  ID                      id-at-attributeCertificate
}

aACertificate ATTRIBUTE ::= {
  WITH SYNTAX             AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  ID                      id-at-aACertificate
}

attributeDescriptorCertificate ATTRIBUTE ::= {
  WITH SYNTAX             AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  ID                      id-at-attributeDescriptorCertificate
}

attributeCertificateRevocationList ATTRIBUTE ::= {
  WITH SYNTAX             CertificateList
  EQUALITY MATCHING RULE  certificateListExactMatch
  ID                      id-at-attributeCertificateRevocationList
}

attributeAuthorityRevocationList ATTRIBUTE ::= {
  WITH SYNTAX             CertificateList
  EQUALITY MATCHING RULE  certificateListExactMatch
  ID                      id-at-attributeAuthorityRevocationList
}

delegationPath ATTRIBUTE ::= {
  WITH SYNTAX  AttCertPath
  ID           id-at-delegationPath
}

AttCertPath ::= SEQUENCE OF AttributeCertificate

privPolicy ATTRIBUTE ::= {
  WITH SYNTAX  PolicySyntax
  ID           id-at-privPolicy
}

protPrivPolicy ATTRIBUTE ::= {
  WITH SYNTAX             AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  ID                      id-at-protPrivPolicy
}

xmlPrivPolicy ATTRIBUTE ::= {
  WITH SYNTAX  UTF8String --contains XML-encoded privilege policy information
  ID           id-at-xmlPrivPolicy
}

-- Attribute certificate extensions and matching rules
attributeCertificateExactMatch MATCHING-RULE ::= {
  SYNTAX  AttributeCertificateExactAssertion
  ID      id-mr-attributeCertificateExactMatch
}

AttributeCertificateExactAssertion ::= SEQUENCE {
  serialNumber  CertificateSerialNumber,
  issuer        AttCertIssuer,
  ...
}

attributeCertificateMatch MATCHING-RULE ::= {
  SYNTAX  AttributeCertificateAssertion
  ID      id-mr-attributeCertificateMatch
```

```
}

AttributeCertificateAssertion ::= SEQUENCE {
  holder
    [0]  CHOICE {baseCertificateID  [0]  IssuerSerial,
                 holderName         [1]  GeneralNames,
                 ...} OPTIONAL,
  issuer           [1]  GeneralNames OPTIONAL,
  attCertValidity  [2]  GeneralizedTime OPTIONAL,
  attType          [3]  SET OF AttributeType OPTIONAL,
  ...
}

-- At least one component of the sequence shall be present
holderIssuerMatch MATCHING-RULE ::= {
  SYNTAX  HolderIssuerAssertion
  ID      id-mr-holderIssuerMatch
}

HolderIssuerAssertion ::= SEQUENCE {
  holder  [0]  Holder OPTIONAL,
  issuer  [1]  AttCertIssuer OPTIONAL,
  ...
}

delegationPathMatch MATCHING-RULE ::= {
  SYNTAX  DelMatchSyntax
  ID      id-mr-delegationPathMatch
}

DelMatchSyntax ::= SEQUENCE {firstIssuer  AttCertIssuer,
                             lastHolder   Holder,
                             ...
}

extensionPresenceMatch MATCHING-RULE ::= {
  SYNTAX  EXTENSION.&id
  ID      id-mr-extensionPresenceMatch
}

-- object identifier assignments
-- object classes
id-oc-pmiUser OBJECT IDENTIFIER ::=
  {id-oc 24}

id-oc-pmiAA OBJECT IDENTIFIER ::= {id-oc 25}

id-oc-pmiSOA OBJECT IDENTIFIER ::= {id-oc 26}

id-oc-attCertCRLDistributionPts OBJECT IDENTIFIER ::= {id-oc 27}

id-oc-privilegePolicy OBJECT IDENTIFIER ::= {id-oc 32}

id-oc-pmiDelegationPath OBJECT IDENTIFIER ::= {id-oc 33}

id-oc-protectedPrivilegePolicy OBJECT IDENTIFIER ::= {id-oc 34}

-- directory attributes
id-at-attributeCertificate OBJECT IDENTIFIER ::=
  {id-at 58}

id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::= {id-at 59}

id-at-aACertificate OBJECT IDENTIFIER ::= {id-at 61}

id-at-attributeDescriptorCertificate OBJECT IDENTIFIER ::= {id-at 62}

id-at-attributeAuthorityRevocationList OBJECT IDENTIFIER ::= {id-at 63}
```

```
id-at-privPolicy OBJECT IDENTIFIER ::= {id-at 71}

id-at-role OBJECT IDENTIFIER ::= {id-at 72}

id-at-delegationPath OBJECT IDENTIFIER ::= {id-at 73}

id-at-protPrivPolicy OBJECT IDENTIFIER ::= {id-at 74}

id-at-xMLPrivilegeInfo OBJECT IDENTIFIER ::= {id-at 75}

id-at-xmlPrivPolicy OBJECT IDENTIFIER ::= {id-at 76}

id-at-permission OBJECT IDENTIFIER ::= {id-at 82}

-- attribute certificate extensions
id-ce-authorityAttributeIdentifier OBJECT IDENTIFIER ::=
  {id-ce 38}

id-ce-roleSpecCertIdentifier OBJECT IDENTIFIER ::= {id-ce 39}

id-ce-basicAttConstraints OBJECT IDENTIFIER ::= {id-ce 41}

id-ce-delegatedNameConstraints OBJECT IDENTIFIER ::= {id-ce 42}

id-ce-timeSpecification OBJECT IDENTIFIER ::= {id-ce 43}

id-ce-attributeDescriptor OBJECT IDENTIFIER ::= {id-ce 48}

id-ce-userNotice OBJECT IDENTIFIER ::= {id-ce 49}

id-ce-sOAIdentifier OBJECT IDENTIFIER ::= {id-ce 50}

id-ce-acceptableCertPolicies OBJECT IDENTIFIER ::= {id-ce 52}

id-ce-targetInformation OBJECT IDENTIFIER ::= {id-ce 55}

id-ce-noRevAvail OBJECT IDENTIFIER ::= {id-ce 56}

id-ce-acceptablePrivilegePolicies OBJECT IDENTIFIER ::= {id-ce 57}

id-ce-indirectIssuer OBJECT IDENTIFIER ::= {id-ce 61}

id-ce-noAssertion OBJECT IDENTIFIER ::= {id-ce 62}

id-ce-issuedOnBehalfOf OBJECT IDENTIFIER ::= {id-ce 64}

id-ce-singleUse OBJECT IDENTIFIER ::= {id-ce 65}

id-ce-groupAC OBJECT IDENTIFIER ::= {id-ce 66}

id-ce-allowedAttAss OBJECT IDENTIFIER ::= {id-ce 67}

id-ce-attributeMappings OBJECT IDENTIFIER ::= {id-ce 68}

id-ce-holderNameConstraints OBJECT IDENTIFIER ::= {id-ce 69}

-- PMI matching rules
id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::=
  {id-mr 42}

id-mr-attributeCertificateExactMatch OBJECT IDENTIFIER ::= {id-mr 45}

id-mr-holderIssuerMatch OBJECT IDENTIFIER ::= {id-mr 46}

id-mr-authAttIdMatch OBJECT IDENTIFIER ::= {id-mr 53}

id-mr-roleSpecCertIdMatch OBJECT IDENTIFIER ::= {id-mr 54}
```

```
id-mr-basicAttConstraintsMatch OBJECT IDENTIFIER ::= {id-mr 55}

id-mr-delegatedNameConstraintsMatch OBJECT IDENTIFIER ::= {id-mr 56}

id-mr-timeSpecMatch OBJECT IDENTIFIER ::= {id-mr 57}

id-mr-attDescriptorMatch OBJECT IDENTIFIER ::= {id-mr 58}

id-mr-acceptableCertPoliciesMatch OBJECT IDENTIFIER ::= {id-mr 59}

id-mr-delegationPathMatch OBJECT IDENTIFIER ::= {id-mr 61}

id-mr-sOAIdentifierMatch OBJECT IDENTIFIER ::= {id-mr 66}

id-mr-extensionPresenceMatch OBJECT IDENTIFIER ::= {id-mr 67}

id-mr-dualStringMatch OBJECT IDENTIFIER ::= {id-mr 69}

END -- AttributeCertificateDefinitions
```

ISO/IEC 9594-9 : 2008, Information Technology - Open systems Interconnection - The Directory: Replication

Working draft for Amendment 1: Communications support enhancements

Annex A

Directory shadow abstract service in ASN.1

Replace the ASN.1 module in Annex A with the following

```
DirectoryShadowAbstractService {joint-iso-itu-t ds(5) module(1)
  directoryShadowAbstractService(15) 6} DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use in the other ASN.1
modules contained
-- within the Directory Specifications, and for the use of other applications which will
use them to access
-- directory services. Other applications may use them for their own purposes, but this
will not constrain
-- extensions and modifications needed to maintain or improve the directory service.
IMPORTS
  -- from ITU-T Rec. X.501 | ISO/IEC 9594-2
  commonProtocolSpecification, directoryAbstractService,
    directoryOperationalBindingTypes, informationFramework,
    directoryOSIProtocols, distributedOperations, dsaOperationalAttributeTypes,
    enhancedSecurity, opBindingManagement
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
      usefulDefinitions(0) 6}
  Attribute{}, AttributeType, CONTEXT, DistinguishedName,
    RelativeDistinguishedName, SubtreeSpecification, SupportedAttributes
    FROM InformationFramework informationFramework
  OPERATIONAL-BINDING, OperationalBindingID
```

```
    FROM OperationalBindingManagement opBindingManagement
  DSEType, SupplierAndConsumers
    FROM DSAOperationalAttributeTypes dsaOperationalAttributeTypes
  OPTIONALLY-PROTECTED{}, OPTIONALLY-PROTECTED-SEQ{}
    FROM EnhancedSecurity enhancedSecurity
  -- from ITU-T Rec. X.511 | ISO/IEC 9594-3
  CommonResultsSeq, ContextSelection, directoryBind, EntryModification,
    SecurityParameters
    FROM DirectoryAbstractService directoryAbstractService
  -- from ITU-T Rec. X.518 | ISO/IEC 9594-4
  AccessPoint
    FROM DistributedOperations distributedOperations
  -- from ITU-T Rec. X.519 | ISO/IEC 9594-5
  id-op-binding-shadow
    FROM DirectoryOperationalBindingTypes directoryOperationalBindingTypes
  shadowConsumerInitiatedAC, shadowSupplierInitiatedAC
    FROM DirectoryOSIProtocols directoryOSIProtocols
  ERROR, OPERATION, id-errcode-shadowError, id-opcode-coordinateShadowUpdate,
    id-opcode-requestShadowUpdate, id-opcode-updateShadow
    FROM CommonProtocolSpecification commonProtocolSpecification;

-- bind operation
dSAShadowBind OPERATION ::= directoryBind

-- shadow operational binding
shadowOperationalBinding OPERATIONAL-BINDING ::= {
  AGREEMENT             ShadowingAgreementInfo
  APPLICATION CONTEXTS
    {{shadowSupplierInitiatedAC
      APPLIES TO  {All-operations-supplier-initiated}} |
      {shadowConsumerInitiatedAC
       APPLIES TO  {All-operations-consumer-initiated}}}
  ASYMMETRIC ROLE-A
    { -- shadow supplier roleESTABLISHMENT-INITIATOR  TRUE
                            ESTABLISHMENT-PARAMETER  NULL
                            MODIFICATION-INITIATOR   TRUE
                            TERMINATION-INITIATOR    TRUE}
  ROLE-B
    { -- shadow consumer roleESTABLISHMENT-INITIATOR  TRUE
                            ESTABLISHMENT-PARAMETER  NULL
                            MODIFICATION-INITIATOR   TRUE
                            MODIFICATION-PARAMETER   ModificationParameter
                            TERMINATION-INITIATOR    TRUE}
  ID                    id-op-binding-shadow
}

-- types
ModificationParameter ::= SEQUENCE {
  secondaryShadows  SET OF SupplierAndConsumers,
  ...
}

AgreementID ::= OperationalBindingID

ShadowingAgreementInfo ::= SEQUENCE {
  shadowSubject     UnitOfReplication,
  updateMode        UpdateMode DEFAULT supplierInitiated:onChange:TRUE,
  master            AccessPoint OPTIONAL,
  secondaryShadows  [2]  BOOLEAN DEFAULT FALSE
}

UnitOfReplication ::= SEQUENCE {
  area              AreaSpecification,
  attributes        AttributeSelection,
  knowledge         Knowledge OPTIONAL,
  subordinates      BOOLEAN DEFAULT FALSE,
  contextSelection  ContextSelection OPTIONAL,
  supplyContexts
```

```
    [0]  CHOICE {allContexts       NULL,
                 selectedContexts  SET SIZE (1..MAX) OF CONTEXT.&id,
                 ...
  } OPTIONAL
}

AreaSpecification ::= SEQUENCE {
  contextPrefix    DistinguishedName,
  replicationArea  SubtreeSpecification,
  ...
}

Knowledge ::= SEQUENCE {
  knowledgeType      ENUMERATED {master(0), shadow(1), both(2)},
  extendedKnowledge  BOOLEAN DEFAULT FALSE,
  ...
}

AttributeSelection ::= SET OF ClassAttributeSelection

ClassAttributeSelection ::= SEQUENCE {
  class            OBJECT IDENTIFIER OPTIONAL,
  classAttributes  ClassAttributes DEFAULT allAttributes:NULL
}

ClassAttributes ::= CHOICE {
  allAttributes  NULL,
  include        [0]  AttributeTypes,
  exclude        [1]  AttributeTypes,
  ...
}

AttributeTypes ::= SET OF AttributeType

UpdateMode ::= CHOICE {
  supplierInitiated  [0]  SupplierUpdateMode,
  consumerInitiated  [1]  ConsumerUpdateMode,
  ...
}

SupplierUpdateMode ::= CHOICE {
  onChange   BOOLEAN,
  scheduled  SchedulingParameters,
  ...
}

ConsumerUpdateMode ::= SchedulingParameters

SchedulingParameters ::= SEQUENCE {
  periodic    PeriodicStrategy OPTIONAL, -- shall be present if othertimes is set to
FALSE
  othertimes  BOOLEAN DEFAULT FALSE,
  ...
}

PeriodicStrategy ::= SEQUENCE {
  beginTime       Time OPTIONAL,
  windowSize      INTEGER,
  updateInterval  INTEGER,
  ...
}

Time ::= GeneralizedTime

-- as per 46.3 b) and c) of ITU-T Rec. X.680 | ISO/IEC 8824-1
-- shadow operations, arguments, and results
All-operations-consumer-initiated OPERATION ::=
  {requestShadowUpdate | updateShadow}
```

```
All-operations-supplier-initiated OPERATION ::=
  {coordinateShadowUpdate | updateShadow}

coordinateShadowUpdate OPERATION ::= {
  ARGUMENT  CoordinateShadowUpdateArgument
  RESULT    CoordinateShadowUpdateResult
  ERRORS    {shadowError}
  CODE      id-opcode-coordinateShadowUpdate
}

CoordinateShadowUpdateArgument ::=
  OPTIONALLY-PROTECTED
    {[0]  SEQUENCE {agreementID         AgreementID,
                    lastUpdate          Time OPTIONAL,
                    updateStrategy
                      CHOICE {standard
                                ENUMERATED {noChanges(0), incremental(1),
                                            total(2),...},
                              other     EXTERNAL,
                              ...},
                    securityParameters  SecurityParameters OPTIONAL,
                    ...}}

CoordinateShadowUpdateResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED{[0]  SEQUENCE {agreementID  AgreementID,
                                        lastUpdate   Time OPTIONAL,
                                        COMPONENTS OF CommonResultsSeq,
                                        ...
      }},
  ...
}

requestShadowUpdate OPERATION ::= {
  ARGUMENT  RequestShadowUpdateArgument
  RESULT    RequestShadowUpdateResult
  ERRORS    {shadowError}
  CODE      id-opcode-requestShadowUpdate
}

RequestShadowUpdateArgument ::=
  OPTIONALLY-PROTECTED
    {[0]  SEQUENCE {agreementID         AgreementID,
                    lastUpdate          Time OPTIONAL,
                    requestedStrategy
                      CHOICE {standard  ENUMERATED {incremental(1), total(2),...},
                              other     EXTERNAL,
                              ...},
                    securityParameters  SecurityParameters OPTIONAL,
                    ...}}

RequestShadowUpdateResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED{[0]  SEQUENCE {agreementID  AgreementID,
                                        lastUpdate   Time OPTIONAL,
                                        COMPONENTS OF CommonResultsSeq,
                                        ...
      }},
  ...
}

updateShadow OPERATION ::= {
  ARGUMENT  UpdateShadowArgument
  RESULT    UpdateShadowResult
  ERRORS    {shadowError}
```

```
  CODE      id-opcode-updateShadow
}

UpdateShadowArgument ::=
  OPTIONALLY-PROTECTED
    {[0]  SEQUENCE {agreementID         AgreementID,
                    updateTime          Time,
                    updateWindow        UpdateWindow OPTIONAL,
                    updatedInfo         RefreshInformation,
                    securityParameters  SecurityParameters OPTIONAL,
                    ...}}

UpdateShadowResult ::= CHOICE {
  null         NULL,
  information
    OPTIONALLY-PROTECTED{[0]  SEQUENCE {agreementID  AgreementID,
                                        lastUpdate   Time OPTIONAL,
                                        COMPONENTS OF CommonResultsSeq,
                                        ...
      }},
  ...
}

UpdateWindow ::= SEQUENCE {start  Time,
                           stop   Time,
                           ...
}

RefreshInformation ::= CHOICE {
  noRefresh      NULL,
  total          [0]  TotalRefresh,
  incremental    [1]  IncrementalRefresh,
  otherStrategy  EXTERNAL,
  ...
}

TotalRefresh ::= SEQUENCE {
  sDSE     SDSEContent OPTIONAL,
  subtree  SET SIZE (1..MAX) OF Subtree OPTIONAL,
  ...
}

SDSEContent ::= SEQUENCE {
  sDSEType          SDSEType,
  subComplete       [0]  BOOLEAN DEFAULT FALSE,
  attComplete       [1]  BOOLEAN OPTIONAL,
  attributes        SET OF Attribute{{SupportedAttributes}},
  attValIncomplete  SET OF AttributeType DEFAULT {},
  ...
}

SDSEType ::= DSEType

Subtree ::= SEQUENCE {
  rdn  RelativeDistinguishedName,
  COMPONENTS OF TotalRefresh,
  ...
}

IncrementalRefresh ::= SEQUENCE OF IncrementalStepRefresh

IncrementalStepRefresh ::= SEQUENCE {
  sDSEChanges
    CHOICE {add     [0]  SDSEContent,
            remove  NULL,
            modify  [1]  ContentChange,
            ...} OPTIONAL,
  subordinateUpdates  SEQUENCE SIZE (1..MAX) OF SubordinateChanges OPTIONAL
```

```
}

ContentChange ::= SEQUENCE {
  rename
    CHOICE {newRDN  RelativeDistinguishedName,
            newDN   DistinguishedName} OPTIONAL,
  attributeChanges
    CHOICE {replace  [0]  SET SIZE (1..MAX) OF Attribute{{SupportedAttributes}},
            changes  [1]  SEQUENCE SIZE (1..MAX) OF EntryModification} OPTIONAL,
  sDSEType          SDSEType,
  subComplete       [2]  BOOLEAN DEFAULT FALSE,
  attComplete       [3]  BOOLEAN OPTIONAL,
  attValIncomplete  SET OF AttributeType DEFAULT {},
  ...
}

SubordinateChanges ::= SEQUENCE {
  subordinate  RelativeDistinguishedName,
  changes      IncrementalStepRefresh,
  ...
}

-- errors and parameters
shadowError ERROR ::= {
  PARAMETER OPTIONALLY-PROTECTED-SEQ
    {SEQUENCE {problem       ShadowProblem,
               lastUpdate    Time OPTIONAL,
               updateWindow  UpdateWindow OPTIONAL,
               COMPONENTS OF CommonResultsSeq,
               ...}}
  CODE                                id-errcode-shadowError
}

ShadowProblem ::= INTEGER {
  invalidAgreementID(1), inactiveAgreement(2), invalidInformationReceived(3),
  unsupportedStrategy(4), missedPrevious(5), fullUpdateRequired(6),
  unwillingToPerform(7), unsuitableTiming(8), updateAlreadyReceived(9),
  invalidSequencing(10), insufficientResources(11)}

END -- DirectoryShadowAbstractService
```