INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION
STANDARDIZATION SECTOR

STUDY PERIOD 2001 - 2004

COM 7-267-E
March 2001
Original: English

Question: 12/7

Texte disponible seulement en
Text available only in
Texto disponible solamente en
} **E**

STUDY GROUP 7 – CONTRIBUTION xxx

SOURCE: ITU-T RAPPORTEUR'S GROUP ON DIRECTORY (Q.12/7)

TITLE: DIRECTORY IMPLEMENTOR'S GUIDE - VERSION 14 - MARCH 2001

Note: This version applies to the 2nd (1993|1995), 3rd (1997|1998), and 4ht (2000/2001) editions of the ITU-T. X.500-series Recommendations and the ISO/IEC 9594 International Standards. It includes all approved and draft corrigenda to the three editions. Readers still using the 1st (1988|1990) edition are advised to keep version 9 of the Directory Implementor's Guide as that is the last version that contains corrections to the 1st edition text. This version will be the last implementor's guide for the 2nd edition. Readers still using the 2nd edition are advised to keep this document.

Agreed at the 2 February 2001 meeting of ITU-T Study Group 7.

***Contact:** Hoyt L. Kesterson II, ISO/IEC
Tel: +1 602 316 1985
Fax: +1 602 978 6750
E-mail: hoytkesterson@earthlink.net

Contents

1 Introduction

1.1 Background

This Guide is a compilation of reported defects and their resolutions to the 2nd (1993), 3rd (1997), and 4th (2000/2001) editions of the ITU X.500 Recommendations and ISO/IEC 9594 Standards. It includes all approved corrigenda, and may include draft corrigenda, to the editions of the Directory specification. It is intended to be an additional authoritative source of information for implementors to be read in conjunction with the Recommendations / Standards themselves.

This Guide itself is not an ITU-T Recommendation or ISO/IEC Standard. However, the appendixes of the Guide reproduce approved Technical Corrigenda, which are formal corrections to the Directory specifications. They may also include draft Technical Corrigenda which have no formal standing and which may be overturned or altered during the ballot process.

1.2 Scope of the Guide

The Guide records the resolution of defects in the following categories:

- editorial errors
- technical errors such as omissions or inconsistencies
- ambiguities

Note: This Guide does not address proposed additions, deletions, or modifications to the Recommendations or Standard that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in the normal way through contributions by national delegates to Question 12 within Study Group 7 of the ITU-T or JTC 1/SC 6/WG 7 Directory group of the ISO/IEC.

1.3 Contacts and Distribution of the Guide

This Guide is distributed through ITU-T Meeting Reports and White Paper contributions, and ISO/IEC JTC1/ SC6 N-series documents. It is also available on-line from the ITU (http://www.itu.int) and from a server maintained by the ISO Rapporteur for Directory (ftp://ftp.bull.com/pub/OSIdirectory/) .

Contacts:

ITU Rapporteur for Q.12/7 Directory Systems 2001-2004

Erik Andersen
CEN/ISSS/WS-DIR
Copenhagen Denmark
Fax: +45 39 45 07 77
E-mail: era.als@get2net.dk

ISO/IEC Directory Rapporteur and International Defect Report Editor & Editor - Directory Implementor's Guide

Hoyt L. Kesterson II
7625 West Villa Rita Drive
Glendale, Arizona 85318
U.S.A.
Fax: +1 602 978 6750

E-mail: hoytkesterson@earthlink.net

ISO/IEC JTC 1/SC 6

Jooran Lee
SC6 Secretariat
Korean Standards Association
#13-31 Yoido-dong, Youngdeungpo-gu
Seoul, 150-010
Republic of Korea
Fax: +82 2 369 8349
E-mail: secretariat@jtc1sc06.org

2 Defect Report and Resolution Procedures

2.1 Submission of Defects

Any implementor of the 1997 or 2000/2001 editions of the X.500 Recommendations or the ISO/IEC International Standard 9594 is invited to submit a Directory defect report using the form found in Appendix D of the guide. The defect report should be submitted to the appropriate National Defect Report Editor, listed in Appendix F. Each form should cover a single defect. It is important that the form is completed accurately, especially the sections that relate to the base material against which the defect report is being raised.

2.2 Resolution of Defects

A collaborative Directory Defect Resolution Committee has been established to resolve reported defects. In the case of most countries, a single representative has been nominated to the committee from the ITU Administration and the ISO/IEC JTC 1 National Body.

Following agreement on a resolution, within the collaborative Defect Resolution Committee, the proposed resolution may require approval via ballot of ISO/IEC and the ITU.

Please note that no individual responses can be given to those submitting reports, and that the procedure is not intended as a consulting service.

3. Guide to Appendixes

The six appendixes of this Guide are organized as follows:

Appendix A is a collection of the approved and draft Technical Corrigenda to the 2nd edition of the Directory specifications. The Technical Corrigenda are numbered from 1 (as for the 1st edition). Approved Technical Corrigenda have been approved by an ISO/IEC ballot and await ITU-T Resolution 1 approval. All corrigenda have been approved by ITU-T Study Group 7, though draft Technical Corrigenda are subject to change through the ISO/IEC ballot. The Directory specifications are arranged in the ISO/IEC order (Parts 1 to 9).

Appendix B is a collection of the approved and draft Technical Corrigenda to the 3rd edition of the Directory specifications. The Directory specifications are arranged in the ISO/IEC order (Parts 1 to 10). Note that this is the last version of the implementor's Guide that will contain TCs for the 2nd edition.

Appendix C is a collection of the approved and draft Technical Corrigenda to the 4th edition of the Directory specifications. The Directory specifications are arranged in the ISO/IEC order (Parts 1 to 10).

Appendix D is a summary of the Defect Reports to the 1993, 1997, and 2000 editions. Defect reports up to and including 074 apply to the 1988 edition only, and are not documented in this version of the Implementor's Guide — see Version 9. That version is the last version of the implementor's guide that document defects against the 1993 edition.

Appendix E is a pro forma defect reporting form. This form, or one like it, should be used for reporting defects. The defect should be submitted together with a electronic copy to ease the editor's task.

Appendix F is a list of Defect Editors with their contact information.

Appendix A

Technical Corrigenda to Rec. X.500 (1993) | ISO/IEC 9594 : 1995 Edition 2

Summary of Edition 2 Technical Corrigenda

ITU-T Rec. X.500 (1993) | ISO/IEC 9594-1:1995

— none

ITU-T Rec. X.501 (1993) | ISO/IEC 9594-2:1995

— Technical Corrigendum 1 (covering resolutions to defect reports 088, 089, 090, 091, 102, 104, 125)

— Technical Corrigendum 2 (covering resolutions to defect reports 134, 136, 140, 143, 144, 145, 147, 149, 171, 172, 174)

— Technical Corrigendum 3 (covering resolutions to defect reports 173, 179, 189, 205)

— Technical Corrigendum 4 (covering resolutions to defect report 211)

ITU-T Rec. X.511 (1993) | ISO/IEC 9594-3:1995

— Technical Corrigendum 1 (covering resolutions to defect report 085)

— Technical Corrigendum 2 (covering resolutions to defect reports 104, 119, 133, 137, 138, 148, 150, 175)

— Technical Corrigendum 3 (covering resolutions to defect reports 166, 179, 188,202,206)

— Technical Corrigendum 4 (covering resolutions to defect report 211)

ITU-T Rec. X.518 (1993) | ISO/IEC 9594-4:1995

— Technical Corrigendum 1 (covering resolutions to defect reports 094, 106, 108, 109, 111, 112, 113, 114, 115)

— Technical Corrigendum 2 (covering resolutions to defect reports 116, 117, 118, 119, 120, 121, 130, 152, 153, 154, 155, 156, 158, 160, 161, 165, 167)

— Technical Corrigendum 3 (covering resolutions to defect reports 157,159, 162, 180, 190, 198, 206, 209)

— Technical Corrigendum 4 (covering resolutions to defect report 211)

ITU-T Rec. X.519 (1993) | ISO/IEC 9594-5:1995

— Technical Corrigendum 1 (covering resolutions to defect reports 075, 124)

— Technical Corrigendum 2 (covering resolutions to defect reports 127, 139)

ITU-T Rec. X.520 (1993) | ISO/IEC 9594-6:1995

— Technical Corrigendum 1 (covering resolutions to defect reports 076, 122, 127)

— Technical Corrigendum 2 (covering resolutions to defect reports 135, 146)

— Technical Corrigendum 3 (covering resolutions to defect report 211)

ITU-T Rec. X.521 (1993) | ISO/IEC 9594-7:1995

— none

ITU-T Rec. X.509 (1993) | ISO/IEC 9594-8:1995

- Technical Corrigendum 1 (covering resolutions to defect report 128)
- Technical Corrigendum 2 (covering resolutions to defect reports 077, 078, 083, 084)
- Technical Corrigendum 3 (covering resolutions to defect reports 80, 92, 100, 177, 183, 194, 196)

ITU-T Rec. X.525 (1993) | ISO/IEC 9594-9:1995

- Technical Corrigendum 1 (covering resolutions to defect reports 097, 099, 123)
- Technical Corrigendum 2 (covering resolutions to defect report 132, 141, 142)
- Technical Corrigendum 3 (covering resolutions to defect reports 182, 186)

Recommendation X.501 (1993) | ISO/IEC 9594-2:1995

Information processing systems - Open Systems Interconnection - The Directory - Models

TECHNICAL CORRIGENDUM 1

(defect reports 088, 089, 090, 091, 102, 125)
Page 41

Clause 12.6.5

Add the following new paragraph to the end of 12.6.5:

> If an entry which is itself a subschema administrative point is not included for the purposes of subschema administration in its subschema subentry then the subschema from the immediately superior subschema administrative area is used to govern the entry.

Clause 12.6.6

Replace item c) in 12.6.6 with the following text:

> c) the **superiorStructureRules** component identifies permitted superior structure rules for entries governed by the rule. If this component is omitted, then the DIT structure rule applies to a subschema administrative point.

Replace the ASN.1 specification of **STRUCTURE-RULE** with:

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

Page 50

Clause 14.7.3

Replace the paragraph “The **information** component …” with:

> The **description** component contains a natural language description of the algorithms associated with the rule.
>
> The **information** component contains the ASN.1 definition of the assertion syntax of the rule.

Page 96

Clause 24.3

In the ASN.1 specification of **ModifyOperationalBindingArgument**, replace the **newAgreement** component with:

```
newAgreement       [7]      OPERATIONAL-BINDING&Agreement
                            ({OpBindingSet}{@binding Type})  OPTIONAL,
```

Page 98

Clause 24.5

Replace the text in item a) with:

a) **invalidID**: The operational binding ID given in the request is not known by the receiving DSA or is in the wrong state for the requested operation.

Page 106

Annex B

Replace the definition of **STRUCTURE-RULE** with the amended definition shown above for clause 12.6.6

Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 Technical Corrigendum 2

(defect reports 134, 136, 143, 144, 145, 147, 149, 171, 172, 174)

This corrects the defect reported in defect report 9594/134.

Clause 24.2

Delete the Note that states that only the **identifier** component of **OperationalBindingID** is present.

Clause 24.4

Replace the paragraph that begins "The identification of the operational binding instance" with the following:

> The identification of the operational binding instance to be terminated is given by **bindingID**. The **version** component present in **bindingID** is ignored.

This corrects the defect reported in defect report 9594/136

Clause 8.2

In the ASN.1 definition of **Attribute**, replace **(1..MAX)** by **(0..MAX)**, i.e.

```
Attribute ::=     SEQUENCE {
          type    ATTRIBUTE.&id ({ SupportedAttributes }),
          values  SET SIZE (0 .. MAX) OF ATTRIBUTE.&TYPE ({
                          SupportedAttributes}{@type})}
```

Replace the paragraph immediately below Note 2 with the following:

> An attribute may be designated as single valued or multi-valued. The Directory shall ensure that single valued attributes have only one value. Attributes in storage shall have at least one value, but may at times appear to have zero values when transferred to or from storage (e.g. because values are hidden by access control).

This corrects the defect reported in defect report 9594/143

Clause 14.7.4

Change the last component of **AttributeTypeInformation** to be:

```
application               AttributeUsage DEFAULT userApplications }
```

This corrects the defect reported in defect report 9594/144

Clause 14.5

Add a new sentence to the end of the first paragraph:

A subschema authority may also create new subschema areas, or remove existing subschema areas by creating or removing subschema subentries, respectively.

This corrects the defect reported in defect report 9594/145

Clause 14.3

Add a new sentence to the end of the paragraph beginning "A single subschema subentry":

The **subtreeSpecification** attribute of a subschema subentry shall specify the whole subschema administrative area, i.e. it shall be an empty sequence.

This corrects the defect reported in defect report 9594/147

Clause 14.7.4

Replace the NOTE by the following:

NOTE — The **attributeSyntax** component is a text string. Identifying an ASN.1 type in a machine processable form is for futher study.

This corrects the defect reported in defect report 9594/149.

Clause 12.5.2

In paragraphs b) and c) of the last list, replace "AVAs" with "AttributeTypeAndValue".

This corrects the defect reported in defect report 9594/171

Clause 12.4.6 b)

Change the text to read:

b) **&Type** is its attribute syntax. This shall be an ASN.1 type, but not a type that contains an **EmbeddedPDV**.

This corrects the defect reported in defect report 9594/172

Clause 2.1

Add the following reference:

— ITU-T Recommendations X.660 (1996) | ISO/IEC 9834-1:1996, Information technology - Open Systems Interconnection - Procedures for the operation of OSI registration authorities: General Procedures.

Clause 12.6.5

Insert the following new paragraphs at the end of 12.6.5:

Entries which are administrative point entries but have no subschema subentry (e.g. newly created administrative point entries), have no governing structure rule. The Directory shall not allow subordinates to be created below such entries until a subschema subentry has been added.

If an entry is converted to a new subschema administrative point, then the governing structure rule of all entries in the new subschema administrative area is automatically changed to that implied by the new subschema.

Clause 13.8

Insert the following new clause at the end of clause 13:

13.8 System schema for first-level subordinates

The Directory enforces the following rules and constraints on entries created immediately subordinate to the DIT root:

— All such entries shall be created as administrative point entries.

— The object class and naming attributes of such entries shall be as specified in ITU-T Rec. X.660 | ISO/IEC 9834-1.

Clause 14.7.9

Change the first paragraph to read:

Every entry in the DIT, with the exception of administrative point entries that have no subschema subentry, has a **governingStrutureRule** operational attribute which indicates the governing structure rule of the entry:

This corrects the defect reported in defect report 9594/174.

Clause 24.2

Add **serviceError** to the ASN.1 **ERRORS** item of **establishOperationlBinding**.

Clause 24.3

Add **serviceError** to the ASN.1 **ERRORS** item of **modifyOperationalBinding**.

Clause 24.4

Add **serviceError** to the ASN.1 **ERRORS** item of **terminateOperationalBinding**.

Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 Technical Corrigendum 3

(defect reports 173, 179, 189, 205)

This corrects the defects reported in defect report 9594/173.

Clause 18.5 First Level DSAs

Change the text of bullet c) the following way:

c) It holds subordinate references (of category master and/or shadow) and non-specific subordinate references (of category master and/or shadow) which account for all the naming contexts immediatly subordinate to the root of the DIT which it does not itself hold.

This corrects the defects reported in defect report 9594/179.

Annex K, Table K-1

In the second column called "Entry protected Item Permissions Required", add the following texts for the Read and the Search operations:

For the Read operation:

"*ReturnDN* for distinguished name"

For the Search Operation:

"*ReturnDN* for each returned distinguished name"

.

This corrects the defects reported in defect report 9594/189.

Clause 24.3 Modify Operational Binding
and **Annex F**

Add OPTIONAL to the ASN.1 of **newAgreement :**

```
newAgreement   [7]     OPERATIONAL-BINDING.&Agreement
                       ({OpBindingSet}{@bindingType}) OPTIONAL,
```

This corrects the defects reported in defect report 9594/205.

Clause 18.3.2. Knowledge Reference Types

Change the first bullet point after "A DSA may hold the following types of knowledge reference:" *to read:*

- superior references;

Clause 18.3.2.1. Superior Reference

Change the title and second sentence to read:

18.3.2.1 Superior References

A superior reference consists of

- the Access Point of a DSA.

Each non-first level DSA (see 18.5) shall maintain at least one superior reference.

Clause 18.4.1. Superior Knowledge

Change the first sentence to read:

Each DSA that is not a first level DSA shall maintain at least one superior reference.

And add the following second sentence:

Additional superior references may be held for operational reasons as alternative paths to the root of the DIT.

Clause 18.5. First Level DSAs

Change the second sentence to read:

“A DSA referenced by other DSAs may itself maintain one or more superior references.”

Change the last sentence to read:

“They therefore may serve as a superior reference for non-first level DSAs.”

Clause19.4.2. DSE Types h)

Change it to read:

h) **supr**: A DSE that holds a specific knowledge attribute to represent the DSAs superior references.

Clause 20.2.1.2. Superior Knowledge

Change the first sentence to plural and the ATTRIBUTE SYNTAX to SET OF, to read:

The **superiorKnowledge** operational attribute type is used by a non-first level DSA to represent its superior references.

```
superiorKnowledge      ATTRIBUTE           ::=     {
                       WITH SYNTAX         SET OF AccessPoint
                       .....
```

Clause 20.2.2.2. Superior Reference

Insert a new second sentence:

Since a **superiorKnowledge** attribute value may contain the access points of several DSAs, it may therefore represent several superior references.

Recommendation X.501 (1993) | ISO/IEC 9594-2:1995
Technical Corrigendum 4

(defect report 211)

This corrects the defects reported in defect report 9594/211.

Clause 24.2

Change the two occurrences of ***UTCTime*** *to* ***Time****:*

Insert the following after the ASN.1 definition of ***Validity***

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

Before a value of **Time** is used in any comparison operation and if the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Clause 24.4

Change ***utctime*** *to* ***Time****:*

Clause 24.5

Change ***utctime*** *to* ***Time****:*

Also make theASN.1 changes to Annex F.

Date: 1995-__-__

Recommendation X.511 (1993) | ISO/IEC 9594-3:1995:

Information processing systems - Open Systems Interconnection - The Directory - Abstract Service Definition

TECHNICAL CORRIGENDUM 1

(defect report 085)

Page 21

Clause 10.1.2

Add the following new paragraph to the end of 10.1.2:

> The **CommonArguments** (see 7.3) include a specification of the service controls applying to the request.

Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 Technical Corrigendum 2

(defect reports 104, 119, 133, 137, 138, 148, 150, 175)

This corrects the defect reported in defect report 9594/104.

Clauses 7.11.1, 10.2.5.1, 11.1.2

In each of these clauses, replace “**aliasedObjectName**” or “**AliasedObjectName**” with “**aliasedEntryName**”.

This corrects the defect reported in defect report 9594/119.

Clause 10.1.3

Append the following to paragraph b):

> See 12.6.

Clause 12.6

Append the following new paragraph:

> Before acting on a continuation reference, the DUA shall check that an identical request to the one that would be generated from the continuation reference has not already been issued as a part of processing the same user request. If it has, the DUA shall not act on the continuation reference. This avoids loops.

This corrects the defect reported in defect report 9594/133.

Clause 7.3.1

Add the following note after the second paragraph of clause 7.3.1:

> NOTE — The first extension is given the identifier 1 and corresponds to bit 1 of the BIT STRING. Bit 0 of the BIT STRING is not used.

This corrects the defect reported in defect report 9594/137

Annex B, Figure B-11

Amend Figure B-11 so that the text ‘incompleteEntry = FALSE’ in the attribute value component of the flowchart reads ‘incompleteEntry = TRUE’.

This corrects the defect reported in defect report 9594/138

Annex B, Figure B.6

In the final question “DiscloseOnError granted to any attributes selected?”, of the flowchart interchange the “Yes” and “No” labels.

This corrects the defect reported in defect report 9594/148

Clause 10.1.3

Change the first paragraph to read:

The request succeeds, subject to access controls, if the **object** is located, regardless of whether there is any subordinate information to return.

Clause 10.2.3

Change the first paragraph to read:

The request succeeds, subject to access controls, if the **baseObject** is located, regardless of whether there are any subordinates to return.

This corrects the defect reported in defect report 9594/150.

Clauses 12.9

Add a **newUpdateProblem** to the ASN.1 definition as follows:

```
noSuchNewSuperior          (8)
```

Add paragraph h) as follows:

h) **noSuchSuperior**. An attempted modifyDN operation names a new superior entry that does not exist.

This corrects the defect reported in defect report 9594/175.

Clauses 7.8.2

Replace the words in "There are no...." in paragraph f) with:

If an item matches for equality, it shall also satisfy an approximate match. Otherwise there are no ...

Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 Technical Corrigendum 3

(defect reports 166, 179, 188, 202, 206)

This corrects the defects reported in defect report 9594/166.

Clause 7.11.1 Alias derefencing

Change the second last sentence of first paragraph of 7.11.1 the following way:

If the DSA chains the request to another DSA and receives back a referral from it, then the access controls shall be applied to the referral if the targetObject in the referral is the same as in the chained request.

This corrects the defects reported in defect report 9594/179.

Annex B, Figure B-4

In the flow chart "return of DN" add under the question "alias name available?/No" an additional question :

"Read operation?"

with the following outputs :

Yes : Name Error
No : *go to next question : "entry corresponds to (base) object of DAP operation?*

Annex B, Figure B-5

In the flow chart "Read Operation" change on the right part the text of the last step of handling "selection empty = yes"
*from "*return Read result*" to "*return Read result or nameError*"* .

This corrects the defects reported in defect report 9594/188.

Clause 11.1.5 Add operation decision points for basic-access-control, bullet 3) , note

Reword the note to read:

“The Add permission must be provided as prescriptiveACI when attempting to add an entry and as prescriptiveACI or subentryACI when attempting to add a subentry.”

This corrects the defects reported in defect report 9594/202.

Clause 7.10 Security Parameters

Replace the paragraph describing **CertificationPath** *with the following*

The **CertificationPath** component is a sequence containing the signer’s user certificate, and, optionally, a sequence of one or more certification authority (CA) certificates. (See clause 8 in ITU-T Rec. X.509 | ISO/IEC 9594-8). The user certificate is used to bind the signer's public key and distinguished name, and may be used to verify the signature on a request argument or response. This parameter shall be present and contain the signer’s user certificate if the request argument or response is signed. Additional certificates may be present and may be used to determine if the signer’s user certificate is valid. Additional certificates are not required if the recipient shares the same certification authority as the signer. If the recipient requires a certification path for validation, and an acceptable parameter is not present, whether the recipient rejects the signature, or attempts to determine a certification path, is a local matter.

Replace the paragraph describing **time** *with the following*

The **time** is the intended expiry time for the validity of the request, response, or error. It is used in conjunction with the random number to enable the detection of replay attacks.

Replace the 1st paragraph describing **random** *with the following*

The **random** value is a number that should be different for each request, response, or error. It is used in conjunction with the time parameter to enable the detection of replay attacks. If sequence integrity is required then the random argument may be used to carry a sequence integrity number as follows: …

This corrects the defects reported in defect report 9594/206.

Clause 10.1.3 List results

In the last paragraph of the clause, change the first part of the first sentence (“When a DUA has requested a protection request of signed, the uncorrelatedListInfo prameter…”) the following way :

“When the DUA has requested a protection request of signed, or if the Directory for other reasons are not able to correlate information, the **uncorrelatedListInfo** parameter...”

Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 Technical Corrigendum 4

(defect report 211)

This corrects the defects reported in defect report 9594/211.

Clause 7.10

Change **UTCTime** *to* **Time***:*

Insert the following after the ASN.1 definition of **ProtectionRequest**

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

Insert the following after the last paragraph of 7.10 .

If the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note —The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Clause 8.1.1

Change the value of **validity** *in the ASN.1 type* **SimpleCredentials** *to*

```
validity    [1]        SET {
        validityPeriod         CHOICE  {
                     COMPONENTS OF ValidityPeriodUTC,  -- UTC when v1
                     COMPONENTS OF ValidityPeriodGT },  -- GT when > v1
        random1     [2]        BIT STRING  OPTIONAL,
        random2     [3]        BIT STRING  OPTIONAL} OPTIONAL,
```

Insert the following after the ASN.1 type **SimpleCredentials** *to*

```
ValidityPeriodUTC          ::=        SET {
        time1         [0]        UTCTime OPTIONAL,
        time2         [1]        UTCTime OPTIONAL }
ValidityPeriodGT  ::=        SET {
        time1         [0]        GeneralizedTime OPTIONAL,
        time2         [1]        GeneralizedTime OPTIONAL }
```

Clause 8.1.2

Insert the following after the second paragraph.

Note — The use of **ValidityPeriodGT** may prevent interworking with implementations unaware of the possibility of choosing either **ValidityPeriodUTC** or **ValidityPeriodGT**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **ValidityPeriodGT** may be used. In no case shall **ValidityPeriodUTC** be used for representing dates beyond 2049.

Change the value of ***time*** *in the ASN.1 type* ***Token*** *to*

```
        time        [2]       Time,
```

Also make theASN.1 changes to Annex A.

Date: 1995-__-__

Recommendation X.518 (1993) | ISO/IEC 9594-4:1995:

Information processing systems - Open Systems Interconnection - The Directory - Procedures for Distributed Operation

TECHNICAL CORRIGENDUM 1

(defect reports 094, 108, 109, 111, 112, 113, 114, 115)

Page 14

Clause 10.4

In item d), delete the word “immediately”.

Page 20

Clause 14.2

Add the following new paragraph to the end of 14.2:

> **Note**: The flowcharts which accompany the procedures are intended to be used as aids towards understanding the procedures. They are not to be considered as being a precise alternative to the textual descriptions. Where there is a disparity between the textual description and the flowchart for a particular procedure, it is intended that the textual description take precedence.

Page 33

Clause 17.3.3.1

Add the following new item b) and then re-label the current items b) - e) as c) - f):

> b) **ChainingArguments.operationProgress** is set to the value of **CommonArguments.operationProgress**.

Page 38

Clause 18.3.1

In step 2), replace the text “continue with step 7)” with “continue at step 5)”.

In step 3) replace the text “If not completed” with “If not **completed**”.

In step 4) replace the text “if the Name Resolution Phase is already completed” with "if **nameResolutionPhase** is **completed**".

In step 6) remove the text “(i.e., is of type shadow)” from the second dash point.

In step 7), 4th dash point, replace the text “continue at step 10)” with “continue at step 8)”.

In step 7), 6th dash point, replace the text “whereas 1988 edition DSAs set **aliasedRDNs** to **i**” with “(whereas 1988 edition DSAs set **aliasedRDNs** to the number of RDNs in **aliasedEntryName**)”. Replace the text “continuing at step 9)” with “continuing at step 1)”.

In step 8) replace the text “if the Name Resolution Phase is already completed” with “if **nameResolutionPhase** is **completed**”.

In step 9) replace the text “If the Name Resolution Phase is completed” with “if **nameResolutionPhase** is **completed**”.

Page 42

Clause 18.3.4.1

Add the following new paragraph to the start of step 8):

> If the operation is **Search** with **searchAliases** set to **TRUE** and the DSE is of type **alias** then if **chainingArguments.excludeShadows** is **FALSE** return **entry suitable**, if it is **TRUE** return **entry unsuitable.**

Replace Figure 12 with the following amended figure:

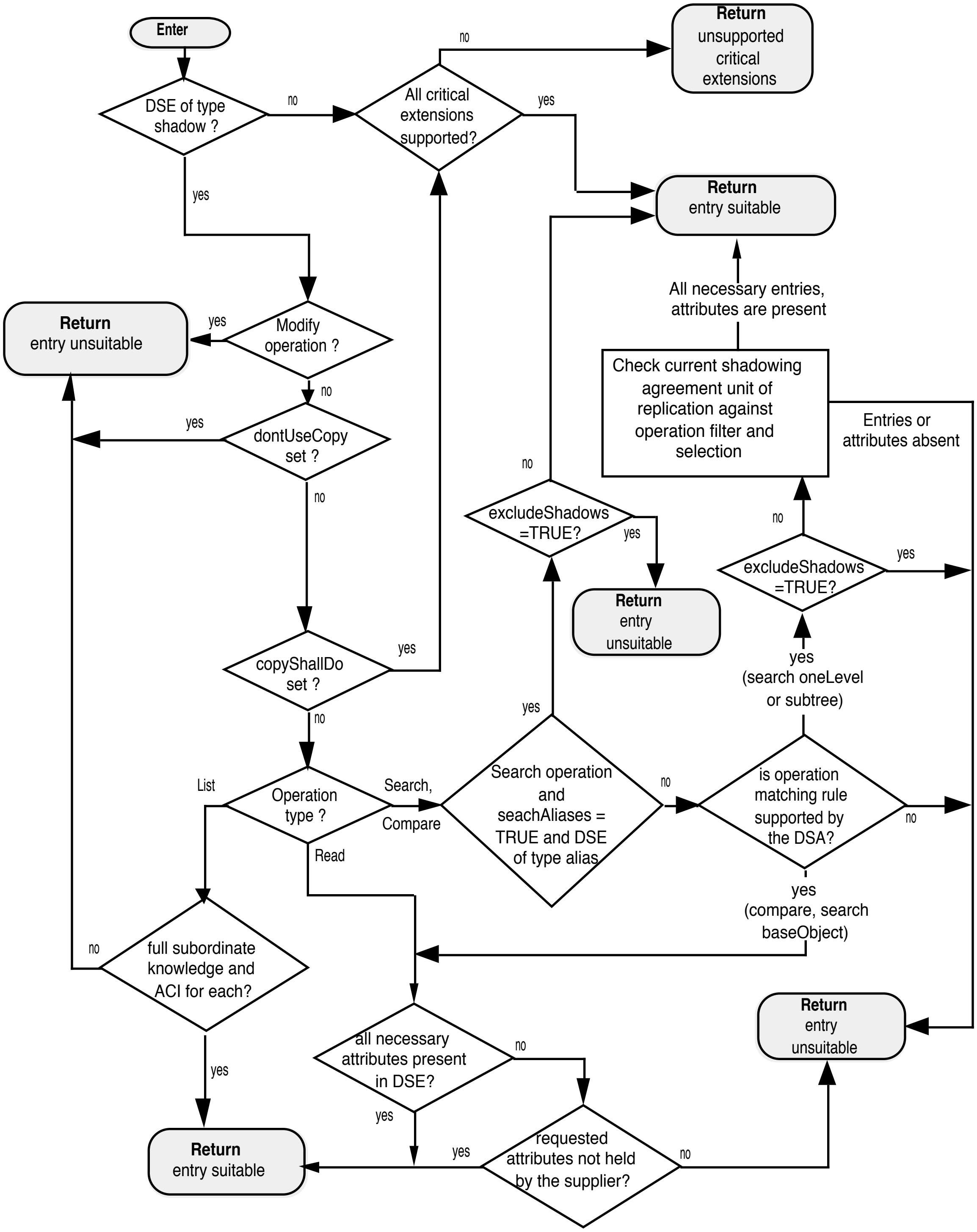

Enter
DSE of type shadow ?
no
All critical extensions supported?
no
Return unsupported critical extensions
yes
Return entry suitable
yes
Modify operation ?
yes
Return entry unsuitable
no
dontUseCopy set ?
yes
no
copyShallDo set ?
yes
no
Operation type ?
List
Search, Compare
Read
Search operation and seachAliases = TRUE and DSE of type alias
yes
no
excludeShadows =TRUE?
no
yes
Return entry unsuitable
is operation matching rule supported by the DSA?
no
yes (search oneLevel or subtree)
excludeShadows =TRUE?
yes
no
Check current shadowing agreement unit of replication against operation filter and selection
All necessary entries, attributes are present
Entries or attributes absent
yes (compare, search baseObject)
Return entry unsuitable
full subordinate knowledge and ACI for each?
no
yes
Return entry suitable
all necessary attributes present in DSE?
no
yes
requested attributes not held by the supplier?
yes
no

Figure 12 — Check Suitability Procedure

Page 47

Clause 19.1.4

Replace the current steps 2) and 3) with the following text:

2) If the operation is either to move an entry or to both move an entry and change its Relative Distinguished Name, go to step 3). If the operation is to only change the Relative Distinguished Name of an entry, go to step 4).

3) The operation shall be performed according to the definition in 11.4.1 of ITU-T Rec. 511 | ISO/IEC 9594-3. If either the old superior, the new superior, the entry or any of its subordinates are not in this DSA, or if the new superior has NSSRs, then the operation shall be rejected with **UpdateError affectsMultipleDSAs**. The DSA shall ensure that no other entry with the new name already exists, otherwise it shall return an **UpdateError** with problem **entryAlreadyExists**. The DSA shall ensure that the new name of the entry conforms to the sub-schema, otherwise it shall return an appropriate **AttributeError** or **UpdateError**. If none of these problems arise then move the entry (changing the RDN if required) and go to step 9).

Page 51, 52

Clause 19.3.1.2.1

Replace the current step 1) with the following text:

1) If the service control **subentry** is set, then go to Step 5), otherwise go to Step 2).

Add the new step 5):

5) For each subentry **e'** immediately subordinate to DSE **e** execute the following steps:

   a) Check the ACI in **e**'. If the ACI disallows listing the RDN of **e**´, then skip this DSE. Otherwise add the RDN of **e'** to **listResult.subordinates** with **aliasEntry** set to **False** and **fromEntry** set according to whether **e'** is a copy.

   b) Check if time, size or administrative limit is exceeded. If so, set **limitProblem** accordingly in **partialOutcomeQualifier** and return.

Add the new step 6):

6) Return to the operation dispatcher.

Page 56

Clause 19.3.2.2.1

In step 4), replace the first line with the following:

If **subset** is **baseObject**, or if **entryOnly** is **TRUE** then continue with this step, otherwise go to step (5).

If one of the following is **TRUE**:

In step 4) substep i), replace the text “go to Step 6)” with “return”.

In step 4), remove substep iii) and replace the final line with:

Return.

In step 7), replace b) with the following:

b) For all cases:

(i) If **subset** is **oneLevel**, set **entryOnly** to **TRUE**.

(ii) Recursively execute **Search Procedure(I)** for target DSE **e'**.

Page 56

Clause 19.3.2.2.2

Replace step 2) with the following:

2) If the DSE is not of type **cp** then ignore it and return to Step 1).

In step 3) remove the first part of the first sentence up to, and including, the comma.

Page 78

Clause 24.1.4.1.1

In the first sentence immediately following the ASN.1 specification of **Vertex**, replace the text up to the first comma with:

The **contextPrefixInfo** component is the sequence of RDNs that form the distinguished name of the immediate superior of the new context prefix

Recommendation X.518 (1993) | ISO/IEC 9594-4:1995 Technical Corrigendum 2

(defect reports 116, 117, 118, 119, 120, 121, 130, 152, 153, 154, 155, 156, 158, 160, 161, 165, 167)

This corrects the defect reported in defect report 9594/116.

Clause 19.3.2.2.3

In steps 2) and 3), replace the words "**targetObject** or **baseObject**" with:

> **targetObject** or **baseObject** or any of the previous values of the target object in **chainingArguments.traceInformation**

This corrects the defect reported in defect report 9594/117.

Clause 20

Add the following text to the end of paragraph 2:

> Within each of these sets there may be continuation references which occur more than once. The sets should be scanned and any duplicates found should be discarded.

Clause 20.4.4

Add the following text to the end of step 3):

> Within each set, remove any duplicates.

This corrects the defect reported in defect report 9594/118.

Clause 20.1.1

Add the following Note after the first paragraph:

> NOTE — Setting **nameResolveOnMaster** to **TRUE** eliminates the possibility of multiple paths during name resolution by (1) ignoring shadow entries and (2) by ensuring that only one DSA may proceed with name resolution in situations where a complex DIT distribution would otherwise permit more than one to proceed. This is achieved by allowing only the DSA holding the master entry corresponding to the first **nextRDNToBeResolved** RDNs of the target object name to continue with name resolution. Any other DSAs will not be able to proceed even though they may hold master entries which match more of the target object name.

This corrects the defect reported in defect report 9594/119.

Clause 16.1.2

Add a new data structure **referralRequests** to the end of the list:

– **referralRequests –** A list of the requests or subrequests which have been chained as a result of executing referrals. Each such request/subrequest is summarised in the form of a **TraceItem**. This list is used by the Loop Avoidance procedure of 15.4.2.

Clause 20.4.5

In Step 5), relabel substep b) as c), update the reference to this clause in a), and add a new substep b):

b) If the request or subrequest to be chained is the result of executing a referral then an extra check for loop avoidance is required. Check if an item with the same **targetObject**, **operationProgress** and target DSA occurs in **referralRequests**. If so then take the action specified in a). If not, then add a new **TraceItem** to **referralRequests** with the following components:

- **targetObject** and **operationProgress** set to the value of the chained request/subrequest;
- **dsa** set to the name of the DSA to which the request/subrequest is to be chained.

This corrects the defect reported in defect report 9594/120.

Clause 21

In each of steps 2) and 3), replace the sentence “Remove all duplicates.” with

Remove all duplicates, giving preference to master information over shadow information.

This corrects the defect reported in defect report 9594/121.

Clause 18.3.1 / Figure 9

In Figure 9, replace the label “cp and other shadow” with two labels “cp and shadow” and “other”, labelling the vertical lines to the left and right of the original label respectively.

Clause 18.3.3

In Step 3), change the value to which **operationProgress.nextRDNToBe-Resolved** is set from **i** to **m**.

Clause 19.3.2.2.1

In Step 1), replace “is a prefix of **e**’s DN” with “is a prefix of the DN of **e**”.

This corrects the defect reported in defect report 9594/130.

Clauses 24.1.4.1.1 and 24.1.4.2

In each of these clauses, add the following Note after the paragraph that defines the **accessPoints** parameter:

NOTE — The master access point within **accessPoints** is the same as that passed in the **accessPoint** parameter of the Establish and Modify Operational Binding operations.

This corrects the defect reported in defect report 9594/140

Clause 24.1.4.2

Add the following to the end of the **SubordinateToSuperior** sequence:

subentries [3] SET OF SubentryInfo OPTIONAL }

Add a new paragraph just before the NOTE:

The **subentries** component of **SubordinateToSuperior** is used by the subordinate to pass subentries containing prescriptive ACI to the superior.

This corrects the defect reported in defect report 9594/152

Clause 12

In the last paragraph, replace reference "14.3" with "12.1" and "14.4" with "12.2",

Clause 12.1

In Note 1, replace reference "14.4" with "12.2".

Clause 19.2

In paragraph 1), replace "clause 10" with "clause 9".

Clause 16.3.9

In the first line, replace "clause 22" with "clause 21".

Clause 24.3.1.2

In step 4), replace "the precedure in 15.7" with "the procedure in 19.1.5".

This corrects the defect reported in defect report 9594/153

Figure 6

Out of the Result Merging Prodecure, make the List Reference Procedure, Search Continuation Reference Procedure and Name Resolution Continuation Reference Procedure arrows double headed. Delete the DSP Request arrows from the Result Merging Procedure.

This corrects the defect reported in defect report 9594/154

Clause 18.2.1

Replace “h) commonArguments.serviceControls.copyShallDo;” with “h) the operation type;”.

Replace “i) commonArguments.serviceControls.dontDereferenceAliases;” with “i) the operation argument.”.

Delete j).

Clause 18.3.4.1

Replace the last dash of the input argument "the serviceControls." by "the operation argument."

This corrects the defect reported in defect report 9594/155

Clause 18.3.1

In steps 4) and 10), replace "subordinate" by "immediate subordinate".

This corrects the defect reported in defect report 9594/156

Clause 19.1.1

In Figure 13, replace "subentry service control set?" by "Subentry?"

This corrects the defect reported in defect report 9594/158

Clause 19.3.2.1.3

Delete clause 19.3.2.1.3.

This corrects the defect reported in defect report 9594/160

Clause 19.3.2.2.1

In step 4) ii) and step 5) ii), delete the sentence “It is a local matter how the appropriate collective attributes are handled...”

This corrects the defect reported in defect report 9594/161

Clause 20.4.4

Replace the second last sentence of the first paragraph with:

Also, the use of exclusions in chaining arguments and of **alreadySearched** in chaining results is defined, as this is an important strategy for search.

This corrects the defect reported in defect report 9594/165

Clause 19.1.5

To 3), add a dash to the end of the chaining arguments as follows:

– timeLimit, as appropriate according to the incoming request.

This corrects the defect reported in defect report 9594/167

Clause 10.3

Change the comment for **aliasesRDNs** in the the ASN.1 definition of **ChainingArguments** to:

-- *absent in 1993 systems*

After f), add the the same note as in X.511 clause 7.3 last paragraph.

Clause 10.10

Add the following comment for **aliasesRDNs** in the the ASN.1 definition of **ChainingArguments**:

-- *absent in 1993 systems*

After b), add the the same note as in X.511 clause 7.3 last paragraph.

Clause 18.3.1

In the 6th dash of 7), replace "1993 edition DSAs set aliasedRDNs to 1,..." with "1993 edition DSAs do not set aliasedRDNs,..."

Recommendation X.518 (1993) I ISO/IEC 9594-4:1995 Technical Corrigendum 3

(defect reports 157, 159, 162, 180, 190, 198, 206, 209)

This corrects the defects reported in defect report 9594/157.

Clause 19.1.4 Modify DN operation

After the first paragraph of bullet 9), add the new paragraph:

"If the entry, alias entry or subentry was within the UnitOfReplication of one or more shadowing agreements held by the DSA, and the superior of the renamed entry, alias entry or subentry is not within this UnitOfReplication, the shadow consumers shall be updated using the procedures of the Directory shadow service specified in ITU-T Rec. X.525|ISO/IEC 9594-9; in this case the shadowed entry and all its subordinates shall be removed.

If the entry, alias entry or subentry was not within the UnitOfReplication of one or more shadowing agreements held by the DSA, and the renamed entry, alias entry or subentry is now within this UnitOfReplication, the shadow consumers shall be updated using the procedures of the Directory shadow service specified in ITU-T Rec. X.525|ISO/IEC 9594-9; in this case the shadowed entry and all its subordinates shall be shadowed."

This corrects the defects reported in defect report 9594/159.

Clause 19.3.2.2.1 Search procedure (I) , 1) b) i)

Replace the whole text of the clause 19.3.2.2.1 1) b) i) with the following text:

i) If **e** is unsuitable, make a **continuationReference** as follows and add it to **SRContinuationList**:
- **targetObject** set to the DN of DSE e
- **operationProgress** with **nameResolutionPhase** set to **proceeding** and **nextRDNtoBeResolved** set to the number of RDNs in e
- all other components of **continuationReference** are unchanged

Then return.

In the note following clause 19.3.2.2.1.1) b) i), remove the brackets with their content.

Clause 18.3.1 Find DSE procedure

Delete step 9)

This corrects the defects reported in defect report 9594/162.

Clause 20.4.5 APInfo procedure, 5) b) second last dash

*Replace "***chainingArguments.exclusions** absent*" by the following text:*

"**chainingArguments.exclusions** is set to either the relevant exclusions for the current target object if called by the Search Continuation Reference procedure, or absent if the APInfo procedure was called by the Name Resolution or the List Continuation procedures."

This corrects the defects reported in defect report 9594/180.

Clause 10.3 Chaining Arguments

Drop bullet g) which is a duplicate of o) and renumber the following clauses. Modify the order of m) n) and) o to o), n) m) which will become with the renumbering :

l) The **entryOnly** ...
m) **uniqueIdentifier**...
n) **authenticationLevel**...

This corrects the defects reported in defect report 9594/190.

Clause 19.3.1.2.2 List procedure (II), step 1b

In bullet 1) add a new step before a) and renumber the following steps:

a) If e´is not an entry or alias, continue with the next immediate subordinate.
b) Check ACI ...

This corrects the defects reported in defect report 9594/198.

Clause 17.3.3.1 DUA request

Insert two new clauses e) and f) into 17.3.3.1 and renumber the existing e) to g), to read:

d) **ChainingArguments.AuthenticationLevel** and **ChaingInArgument.UniqueID** are set according to the local security policy.

e) **ChainingArguments.nameResolveOnMaster** is copied from **CommonArguments.nameResolveOnMaster**.

f) **ChainingArguments.exclusions, ChainingArguments.entryOnly** and **ChainingArguments.referenceType** are copied from **CommonArguments.exclusions, CommonArguments.entryOnly** and **CommonArguments.referenceType** if they are present, otherwise they are omitted.

g) The remaining optional elements of **ChainingArguments** are omitted, with default values being assumed where specified.

.
This corrects the defects reported in defect report 9594/206.

Clause 21 Results Merging procedure

Add the following note after bullet 6) :

> "Note : In case a DSA receives search or list results from other DSAs and such results have parameters unknown to the DSA, the uncorrelated results shall be returned. Otherwise, the DSA shall perform merging, if the search results are not signed.
>
> A DSA which received unsigned, uncorrelated results from a DSA not able to perform consolidation, shall perform merging, if it has the proper knowledge of all parameters of the uncorrelated results."

This corrects the defects reported in defect report 9594/209.

Clause 12.1 Chained operations and Annex A

Modify as follows the ASN.1 of ERRORS :

```
ERRORS        {operation.&Errors Except referrall dsaReferral}
```

Recommendation X.518 (1993) | ISO/IEC 9594-4:1995
Technical Corrigendum 4

(defect reports 211)

This corrects the defects reported in defect report 9594/211.

Clause 10.3

Change **timeLimit** *in* **ChainingArugments** *to:*

```
timeLimit   [9]        Time OPTIONAL,
```

Insert the following after the ASN.1 definition of **ChainingArugments**

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

Add the following to k):

Before a value of **Time** is used in any comparison operation and if the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Also make theASN.1 changes to Annex A.

Date: 1995-__-__

Recommendation X.519 (1993) | ISO/IEC 9594-5:1995

Information processing systems - Open Systems Interconnection - The Directory - Protocol Specifications

TECHNICAL CORRIGENDUM 1

(defect reports 075, 124)

Page 10

Clause 7.1

Add the following note at the end of the clause (just before clause 7.1.1):

Note — The abstract syntaxes defined in this clause that import from module **DirectoryShadowAbstractService** will use a mixture of implicit and explicit tags.

Page __

Clause 9.1.1

Replace (b) with the following:

(b) The bind security level(s) for which conformance is claimed (none, simple, strong — and if simple, then whether without-password, with-password, or with protected-password); and whether the DUA can generate signed arguments or validate signed results.

Clause 9.2.1

Replace (e) with the following, and renumber the remaining items in the list:

(e) If conformance is claimed to the **directoryAccessAC** application context, the bind security level(s) for which conformance is claimed (none, simple, strong — and if simple, then whether without-password, with-password, or with protected-password); whether the DSA can perform originator authentication as defined in [Part 4 | X.518] clause 18.9.1 and if so, whether identity-based or signature-based; and whether the DSA can perform result authentication as defined in [Part 4 | X.518] clause 18.9.2.

(f) If conformance is claimed to the **directorySystemAC** application context, the bind security level(s) for which conformance is claimed (none, simple, strong — and if simple, then whether without-password, with-password, or with protected-password); whether the DSA can perform originator authentication as defined in [Part 4 | X.518] clause 18.9.1 and if so, whether identity-based or signature-based; and whether the DSA can perform result authentication as defined in [Part 4 | X.518] clause 18.9.2.

Recommendation X.519 (1993) | ISO/IEC 9594-5:1995 Technical Corrigendum 2

(defect reports 127, 139)

This corrects the defect reported in defect report 9594/127

Page __

Clause 9.2.1

In statement requirement f), replace the text "...**DirectoryString** conformance is claimed for the **UNIVERSAL STRING** choice." with "...**DirectoryString** conformance is claimed for the choice **BMPString**, **UNIVERSAL STRING**, or both."

This corrects the defect reported in defect report 9594/139

Clause 7.2.3.1

Replace the sentence comprising the third pargraph, "A variant of this operation..." with:

The **ShadowSupplierInitiatedAsynchronousAC** variant of this application context permits the use of asynchronous operations.

Add the following ASN.1 definition following the third paragraph, and update Annex C accordingly:

```
ShadowSupplierInitiatedAsynchronousAC  APPLICATION-CONTEXT          ::=        {
       CONTRACT                                      shadowSupplierContract
       ESTABLISHED BY                    acse
       INFORMATION TRANSFER BY           pData
       ABSTRACT SYNTAXES                 {acse-abstract-syntax |
           directoryShadowAbstractSyntax }
       APPLICATION CONTEXT NAME          id-ac-
           ShadowSupplierInitiatedAsynchronousAC }
```

Clause 7.2.3.2

Replace the sentence comprising the third pargraph, "A variant of this operation..." with:

The **ShadowConsumerInitiatedAsynchronousAC** variant of this application context permits the use of asynchronous operations.

Add the following ASN.1 definition following the third paragraph, and update Annex C accordingly:

```
ShadowConsumerInitiatedAsynchronousAC           APPLICATION-CONTEXT          ::=
           {
       CONTRACT                                      shadowConsumerContract
       ESTABLISHED BY                    acse
       INFORMATION TRANSFER BY           pData
       ABSTRACT SYNTAXES                 {acse-abstract-syntax |
           directoryShadowAbstractSyntax }
       APPLICATION CONTEXT NAME          id-ac-
```

ShadowConsumerInitiatedAsynchronousAC }

Clause 8.1.1.1.2

Amend the text in point d) to read:

For the **DISP**, one of **shadowSupplierInitiatedAC**, **shadowConsumerInitiatedAC**, **shadowSupplierInitiatedAsynchronousAC**, or **shadowConsumerInitiatedAsynchronousAC**.

Clause 9.3.1

Amend the text in point a) to read:

a) the application context(s) for which conformance is claimed in shadow supplier: **shadowSupplierInitiatedAC**, **shadowSupplierInitiatedAsynchronousAC**, and **reliableShadowSupplierInitiatedAC**.

A DSA shall, at a minimum, support either the **shadowSupplierInitiatedAC** or the **shadowConsumerInitiatedAC**. If the DSA suports the **shadowSupplierInitiatedAC**, it may optionally support one or both of the **shadowSupplierInitiatedAsynchronousAC** or **reliableShadowSupplierInitiatedAC**. If the DSA supports the **shadowConsumerInitiatedAC**, it may optionally support one or both of the **shadowConsumerInitiatedAsynchronousAC** or **reliableShadowConsumerInitiatedAC**.

Clause 9.4.1

Amend the text in point a) to read:

a) the application context(s) for which conformance is claimed in shadow consumer: **shadowConsumerInitiatedAC**, **shadowConsumerInitiatedAsynchronousAC**, and **reliableShadowConsumerInitiatedAC**.

A DSA shall, at a minimum, support either the **shadowSupplierInitiatedAC** or the **shadowConsumerInitiatedAC**. If the DSA suports the **shadowSupplierInitiatedAC**, it may optionally support one or both of the **shadowSupplierInitiatedAsynchronousAC** or **reliableShadowSupplierInitiatedAC**. If the DSA supports the **shadowConsumerInitiatedAC**, it may optionally support one or both of the **shadowConsumerInitiatedAsynchronousAC** or **reliableShadowConsumerInitiatedAC**.

Annex C3

Import the following from **ProtocolObjectIdentifiers**:

id-ac-shadowSupplierInitiatedAsynchronousAC
id-ac-shadowConsumerInitiatedAsynchronousAC

Date: 1995-__-__

Recommendation X.520 (1993) | ISO/IEC 9594-6:1995

Information processing systems - Open Systems Interconnection - The Directory - Selected Attribute Types

TECHNICAL CORRIGENDUM 1

(defect reports 076, 122, 126)

Page 3

Clause 5

Replace the ASN.1 specification with:

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

Replace the final paragraph with:

> Some implementations of the Directory do not support **BMPString** or **UniversalString**, and will not be able to generate, match, or display attributes having such a syntax.

Page 15

Clause 6.1.1

In the first paragraph, replace the text “attribute value of type **DirectoryString**” with:

> attribute value of type **PrintableString**, **NumericString**, **TeletexString**, **BMPString**, **UniversalString**, or **DirectoryString**

Page 15 - 17

Clause 6.1.2 - 6.1.6

In the first paragraph, replace the text “attribute value of type **DirectoryString**” with:

> attribute value whose type is one of the ones listed in 6.1.1

Page __

Clause 6.2

Replace the first four paragraphs (up to the words ‘single space character’) with the following:

In the matching rules specified in 6.1.1 through 6.1.11, the following spaces are regarded as not significant:

- leading spaces (i.e. those preceding the first character that is not a space);
- trailing spaces (i.e. those following the last character that is not a space);
- multiple consecutive spaces (these are taken as equivalent to a single space character).

A string consisting entirely of spaces is equivalent to a string containing exactly one space.

Recommendation X.520 (1993) | ISO/IEC 9594-6:1995 Technical Corrigendum 2

(defect reports 135, 146)

This corrects the defect reported in defect report 9594/135.

Page __

Clause 6.3.2

Add the following sentence after the words '... earlier than the presented time.':

UTC times with year values 50 to 99 shall be taken to represent times that are earlier than UTC times with year values 00 to 49.

This corrects the defect reported in defect report 9594/146

Page __

Clause 5.2.3

Replace **ub-name** with **ub-surname** in the ASN.1 definition for **surname**.

Annex A

Replace **ub-name** with **ub-surname** in the ASN.1 definition for **surname**.

Annex C

Replace the definition of **ub-name** with the definition for **ub-surname** as follows:

```
ub-surname          INTEGER         ::=       64
```

Recommendation X.520 (1993) | ISO/IEC 9594-6:1995 Technical Corrigendum 3

(defect reports 211)

This corrects the defects reported in defect report 9594/211.

Clause 6.3.2

Add the following to the last paragraph

The value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Date: 1995-__-__

Recommendation X.509 (1993) | ISO/IEC 9594-8:1995

Information processing systems - Open Systems Interconnection - The Directory - Authentication Framework

TECHNICAL CORRIGENDUM 1

(defect report 128)

Clause 2.1

Add a new reference, as follows:

> CCITT Rec. X.660 (1992) | ISO/IEC 9834-1:1993, Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities: General Procedures.

Clause 8

In the ASN.1 specification for **Certificate**, make the following changes:

- In the comment for **issuerUniqueID**, replace "*must be v2*" with "*must be v2 or v3*"
- In the comment for **subjectUniqueID**, replace "*must be v2*" with "*must be v2 or v3*"
- Add the following as a new element to the end of the sequence:

```
extensions      [3]      Extensions OPTIONAL
                         -- If present, version must be v3 --   }         }
```

In the **Version** production, add a new value "**v3(2)**"

Add the following, immediately below the ASN.1 specification for **SubjectPublicKeyInfo**:

```
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 ordering.

```
Extension ::= SEQUENCE {
     extnId          EXTENSION.&id ({ExtensionSet}),
     critical        BOOLEAN DEFAULT FALSE,
     extnValue       OCTET STRING
                     -- contains a DER encoding of a value of type &ExtnType
                     -- for the extension object identified by extnId -- }

-- Definition of the following information object set is deferred, perhaps to
-- standardized profiles or to protocol implementation conformance statements.

ExtensionSet        EXTENSION      ::=       { ... }
```

The extensions field allows addition of new fields to the structure without modification to the ASN.1 definition. An extension field consists of an extension identifier, a criticality flag, and a canonical encoding of a data value of an ASN.1 type associated with the identified extension. When an implementation processing a certificate does not recognize an extension, if the criticality flag is FALSE, it may ignore that extension. If the criticality flag is TRUE, unrecognized extensions shall cause the structure to be considered invalid, i.e., in a certificate, an unrecognized critical extension would cause validation of a signature using that certificate to fail.

The following object class is used to define specific extensions.

Specificextensions may be defined in ITU-T Recommendations | International Standards or by any organizations which has a need. The object indentifier which identifies an extension shall be defined in accordanc with ITU-T Rec. X.660 | ISO/IEC 9834-1.

```
EXTENSION ::= CLASS
{
    &id               OBJECT IDENTIFIER UNIQUE,
    &ExtnType
}
WITH SYNTAX
{
    SYNTAX            &ExtnType
    IDENTIFIED BY     &id
}
```

Clause 11.2

In the ASN.1 **CertificateList** production, add a new **version** element as the first element of the **SEQUENCE** (ahead of the **signature** element) as follows:

```
version              Version  OPTIONAL,
                     -- if present, version must be v2--
```

In the ASN.1 **CertificateList** production, add **crlExtensions** as a final element of the **CertificateList SEQUENCE** and add **crlEntryExtensions** as the final element of the **revokedCertificates SEQUENCE OF SEQUENCE**, by replacing the last line of the production

```
 revocationDate      UTCTime } OPTIONAL }}
```

with the following:

```
revocationDate       UTCTime,
crlEntryExtensions   Extensions OPTIONAL } OPTIONAL,
crlExtensions        [0]  Extensions OPTIONAL }}
```

Add a new note (note 3) to the list of notes immediately following the ASN.1 CertificateList production as follows:

3 If any extensions included in a **CertificateList** are defined as critical, the version element of the **CertificateList** shall be present. If no extensions defined as critical are included, the version element shall be absent.

4 When an implementation processing a certificate revocation list does not recognize a critical extension in the **crlEntryExtensions** field, it shall assume that, at a minimum, the identified certificate has been revoked and is no longer valid and perform additional actions concerning that revoked certificate as dictated by local policy. When an implementation does not recognize a critical extension in the **crlExtensions** field, it shall assume that identified certificates have been revoked and are no longer valid. However in the latter case, since the list may not be complete, certificates that have not been identified as being revoked cannot be assumed to be valid. In this case local policy shall dictate the action to be taken. In any case local policy may dictate actions in addition to and/or stronger than those stated in this specification.

5 If an extension affects the treatment of the list (e.g. multiple CRLs must be scanned to examine the entire list of revoked certificates, or an entry may represent a range of certificates), then that extension shall be indicated as critical in the **crlExtensions** field regardless of where the extension is placed in the CRL. An extension

indicated in the **crlEntryExtensions** field of an entry shall be placed in that entry and shall affect only the certificate(s) specified in that entry.

Annex A

In the ASN.1 specification for **Certificate**, make the following changes:

- In the comment for **issuerUniqueID**, replace "*must be v2*" with "*must be v2 or v3*"
- In the comment for **subjectUniqueID**, replace "*must be v2*" with "*must be v2 or v3*"
- Add the following as a new element to the end of the sequence:

```
extensions      [3]      Extensions OPTIONAL
                         - If present, version must be v3 --    } }
```

In the **Version** production, add a new value "**v3(2)**"

Add the following, immediately below the ASN.1 specification for **SubjectPublicKeyInfo**:

```
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 ordering.

```
Extension ::= SEQUENCE {
    extnId          EXTENSION.&id ({ExtensionSet}),
    critical        BOOLEAN DEFAULT FALSE,
    extnValue       OCTET STRING
                    -- contains a DER encoding of a value of type &ExtnType
                    -- for the extension object identified by extnId -- }

-- 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 critical component of  Extension.

 ExtensionSet        EXTENSION      ::=      { ... }

EXTENSION ::= CLASS
{
    &id             OBJECT IDENTIFIER UNIQUE,
    &ExtnType
}
WITH SYNTAX
{
    SYNTAX          &ExtnType
    IDENTIFIED BY   &id
}
```

In the ASN.1 **CertificateList** production, add a new **version** element as the first element of the **SEQUENCE** (ahead of the **signature** element) as follows:

```
version             Version  OPTIONAL,
                    -- if present, version must be v2--
```

In the ASN.1 **CertificateList** production, add **crlExtensions** as a final element of the CertificateList SEQUENCE and add crlEntryExtensions as the final element of the **revokedCertificates SEQUENCE OF SEQUENCE**, by replacing the last line of the production **revocationDate UTCTime } OPTIONAL }}** with the following:

```
revocationDate      UTCTime,
crlEntryExtensions  Extensions OPTIONAL } OPTIONAL,
crlExtensions       [0]  Extensions OPTIONAL }}
```

Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 Technical Corrigendum 2

(defect reports 077, 078, 083, 084)

Page 1

Clause 1

In paragraph 5, replace the sentence "The user certificates …" with the following text:

> The user certificates are assumed to be formed by 'off-line' means, and may subsequently be placed in the Directory.

Page 8

Clause 7

In the first paragraph, replace the word "secret" with "private".

Page 17

Clause 11.1

In the second paragraph, replace the word "secret" with "private".

Clause 11.2

In the list a) - c), replace the text in b) with the following text:

> b) If the means of generation of key pairs of 11.1(b) or of 11.1(c) is employed, the user's private key must be transferred to the user in a secure manner.

Page 28

Annex D.4

Add the following text to the end of the second sentence in the second last paragraph of D.4:

> where the first bit is the highest order bit of the first octet of the data block.

Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 Technical Corrigendum 3

(defect reports 080, 092, 100, 177, 183, 194, 196)

This corrects the defects reported in defect reports 9594/080 and 9594/092.

Clause 9

Remove the clause beginning “In the case where only the signature is required” and the existing definition of SIGNATURE, and replace these by the following clause placed after Note 4 (before the clause beginning “In the case where a signature must be appended”):

The signature of some data item is formed by encrypting a shortened or “hashed” transformation of the item, and may be described by the following ASN.1:

```
ENCRYPTED-HASH { ToBeSigned }      ::=           BIT STRING ( CONSTRAINED BY {
    -- must be the result of applying a hashing procedure to the BER-encoded octets --
    -- of a value of -- ToBeSigned -- and then applying an encipherment procedure to those octets -- })
SIGNATURE { ToBeSigned }         ::=        SEQUENCE {
        algorithmIdentifier                 AlgorithmIdentifier,
        encrypted                                   ENCRYPTED-HASH { ToBeSigned }}
```

NOTE 5 — The encryption procedure requires the agreements listed in Note 2, and also agreement as to whether the hashed octets are encrypted directly, or only after further encoding them as a BIT STRING using the ASN.1 BasicEncoding Rules.

Annex A

Replace the definitions of the parameterized type **HASHED** with the definition of **ENCRYPTED-HASH** (from Clause 9)

Change the definition of **SIGNATURE** to that given in the amended Clause 9 and move it to immediately above the definition of **SIGNED**.

This corrects the defect reported in defect reports 9594/100.

Clause 9

Add the following text to the end of clause 9, after the list a) to h):

Generating a distinguished encoding requires the abstract syntax of the data to be encoded to be fully understood. The Directory may be required to sign data or check the signature of data that contains unknown protocol extensions or unknown attribute syntaxes. The Directory shall follow these rules:

— It shall preserve the encoding of received information whose abstract syntax it does not fully know and which it expects to subsequently sign;

— When signing data for sending, it shall send data whose syntax it fully knows with a distinguished encoding and any other data with its preserved encoding, and shall sign the actual encoding it sends;

— When checking signatures in received data, it shall check the signature against the actual data received rather than its conversion of the received data to a distinguished encoding.

This corrects the defect reported in defect report 9594/177.

Page __

Clause 9

Add the following items to the list numbered a) to h) at the end of the clause:

i) the encoding of a UTC time shall be as specified in ITU-T Rec. X.690 Corr. 2 | ISO/IEC 8825-1:1994 Corr. 2;

j) the encoding of a Generalized time shall be as specified in ITU-T Rec. X.690 | ISO/IEC 8825-1:1994.

This corrects the defect reported in defect report 9594/183.

Page __

Clause 8

Insert the following new paragraph after the first paragraph that follows the ASN.1 definition of **ExtensionSet**.

If unknown elements appear within the extension, and the extension is not marked critical, those unknown elements shall be ignored according to the rules of extensiblity documented in 7.5.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5.

Page __

Clause 12.2.2.3

Add to Key Usage BIT STRING

```
encipherOnly (7),
decipherOnly (8) }
```

Add to end of item list:

h) **encipherOnly**: public key agreement key for use only in enciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined);

i) **decipherOnly**: public key agreement key for use only in deciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined);

This corrects the defect reported in defect report 9594/194.

Page __

Clauses 8, 11, 12

Replace every appearance of **UTCTime** in the ASN.1 definitions with **Time**. This will occur twice in the definition of the **Validity** type definition in clause 8. It will occur three times in the definition of the **CertificateList** sequence in 11.2. It occurs once each in the definitions of **CertificateAssertion** in 12.7.2, **CertificateListExactAssertion** in 12.7.5, and **CertificateListAssertion** in 17.7.6. Replace the same definitions in Annex A.

Page __

Clause 8

Insert the following immediately before the ASN.1 definition of the Extensions type in clause 8.

```
Time  ::= CHOICE {
      utcTime               UTCTime,
         generalizedTimeGeneralizedTime }
```

Insert the following immediately after the ASN.1 definition of the **ExtensionSet** type in clause 8.

Before a value of **Time** is used in any comparison operation, e.g. as part of a matching rule in a search, and if the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two digit year field shall be rationalized into a four digit year value as follows:

— If the 2 digit value is 00 through 49 inclusive, the value shall have 2000 added to it.
— If the 2 digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which certificates defined in this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Date: 1995-__-__

Recommendation X.525 (1993) | ISO/IEC 9594-9:1995

Information processing systems - Open Systems Interconnection - The Directory - Replication

TECHNICAL CORRIGENDUM 1

(defect reports 097, 099, 123)

Page 13

Clause 8.2.2.1

Remove the second last paragraph ("If the **ModificationParameter** parameter is present, it is ignored.").

Page 14

Clause 8.3 and Annex A

Replace the ASN.1 specification of **shadowOperationalBinding** with:

```
shadowOperationalBinding OPERATIONAL-BINDING   ::=   {
      AGREEMENT                   ShadowingAgreementInfo
      APPLICATION CONTEXTS {
            { shadowSupplierInitiatedAC
                  APPLIES TO { All-operations-supplier-initiated } } |
            { shadowConsumerInitiatedAC
                  APPLIES TO { All-operations-consumer-initiated } } |
            { reliableShadowSupplierInitiatedAC
                  APPLIES TO { All-operations-supplier-initiated } } |
            { reliableShadowConsumerInitiatedAC
                  APPLIES TO { All-operations-consumer-initiated } } }
      ASYMMETRIC
            ROLE-A      {       -- shadow supplier role
                  ESTABLISHMENT-INITIATORTRUE
                  ESTABLISHMENT-PARAMETER          NULL
                  MODIFICATION-INITIATOR      TRUE
                  TERMINATION-INITIATOR       TRUE }
            ROLE-B      {       -- shadow consumer role
                  ESTABLISHMENT-INITIATORTRUE
                  ESTABLISHMENT-PARAMETER          NULL
                  MODIFICATION-INITIATOR      TRUE
                  MODIFICATION-PARAMETER  ModificationParameter
                  TERMINATION-INITIATOR       TRUE }
      ID    id-op-binding-shadow }
```

Page 28

Clause 12

Replace the last line of the ASN.1 definition of **ShadowingProblem** with the following:

```
invalidSequencing  (10),
insufficientResources         (11))
```

Page 29

Clause 12.1

Add the following item to the list:

k) i**nsufficientResources**: Indicates that the executing DSA has insufficient resources to carry out the operation.

Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 Technical Corrigendum 2

(defect reports 132, 141, 142)

This corrects the defect reported in defect report 9594/132.

Clauses 11.1.1 and 11.2.1

Replace the definition of **lastUpdate** in both clauses with the following:

> The **lastUpdate** argument is the time provided by the shadow supplier in the most recent successful update. It shall be absent if there has been no previous successful update for the shadowing agreement, or if the shadow consumer requires a full update even if there have been no changes to the shadowed information, e.g. to recover from errors.

Clause 11.3.1

Append the following to the paragraph that defines **noRefresh**:

> It shall not be used where the **updateShadow** operation is in response to a **coordinateShadowUpdate** or **refreshShadowUpdate** operation in which the **lastUpdate** argument has been omitted.

This corrects the defect reported in defect report 9594/141.

Clause 9.2

Replace the last sentence of paragraph 3 with:

> The policy information to be included begins at an autonomous administrative point and extends to the replication base entry, but does not include it:

Figures 3 and 4

Replace “Prefix Information” with “Policy Information” in the figures.

This corrects the defect reported in defect report 9594/142.

Clause 9.2

In the text following the ASN.1 definition, add after the description of **area**, and before the description of **SubtreeSpecification**, the following sentence:

> For the case where a DSA is shadowing first level knowledge from a first level DSA, the **contextPrefix** component is empty.

Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 Technical Corrigendum 3

(defect reports 182, 186)

This corrects the defects reported in defect report 9594/182.

Clause 7.2.2.3

Insert as a fourth new paragraph

> If **subordinates** is specified, then the supplier shall send subordinate entries and a subordinate reference, and the SDSEs will be of type **subr**, **entry**, and **cp**. The subordinate entries shall contain attributes according to the attribute selection. In addition, if the supplying DSE is of type **admPoint**, then the SDSE shall additionally be of type **admPoint** and the **administrativeRole** attribute shall be supplied. All appropriate subentries, with only the appropriate information, below the **admPoint** DSE shall also be supplied as SDSEs in the shadowed information.

Clause 9.2 and Annex A

Replace the **UnitOfReplication** *ASN,1 type as follows (thereby adding* **subordinates***):*

```
UnitOfReplication        ::=     SEQUENCE {
        area                             AreaSpecification,
        attributes                       AttributeSelection,
        knowledge                        Knowledge OPTIONAL,
        subordinates                     BOOLEAN DEFAULT FALSE }
```

Insert the following after the description of **knowledgetype**

subordinates is used to indicate that subordinate entries, rather than simply subordinate references, are to be copied to the consumer DSA. **subordinates** may only be **TRUE** if **knowledge** is requested and **extendedKnowledge** is **FALSE**.

This corrects the defects reported in defect report 9594/186.

Clause 7.2.2.2

Append the following to a) in the fifth paragraph

If the **entryACI** operational attribute is present and holds relevant ACI, e.g. naming, then the attribute (containing at least the relevant ACI) shall always be included in the SDSE.

Clause 9.2.4.1

Add a new list element d)

d) If the entry is refined out, the replacement glue SDSE shall contain the necessary access control information.

Delete "prescriptive" from Note 2.

Appendix B

Technical Corrigenda to Rec. X.500 (1997) | ISO/IEC 9594 : 1998 3rd Edition

Summary of 3rd Edition Technical Corrigenda

DTC #	Defect Reports resolved	Ballot Close	Published As	History
ITU-T Rec. X.500 (1997) | ISO/IEC 9594-1:1998				
1-DTC1	228	10 Jan 2001	withdrawn	Erik after Orlando 2000
ITU-T Rec. X.501 (1997) | ISO/IEC 9594-2:1998				
2-DTC1	173, 179, 189, 205		2-TC1	Patrick after Orlando 99
2-DTC2	211		2-TC1	Hoyt after Orlando 99
2-DTC3	229, 230		2-TC2	
2-DTC4	228, 242, 255, 260, 261, 267, 269	10 Jan 2001	2-TC2	Erik after Orlando 2000
ITU-T Rec. X.511 (1997) | ISO/IEC 9594-3:1998				
3-DTC1	166, 179, 188, 202, 206, 217		3-TC1	Patrick after Orlando 99
3-DTC2	211		3-TC1	Hoyt after Orlando 99
3-DTC3	231, 232		3-TC2	

DTC #	Defect Reports resolved	Ballot Close	Published As	History
3-DTC4	247		3-TC2	
3-DTC5	224, 228, 242, 263	10 Jan 2001	3-TC2	Erik after Orlando 2000
ITU-T Rec. X.518 (1997) | ISO/IEC 9594-4:1998				
4-DTC1	157,159,162,180, 190, 198, 206, 209		4-TC1	Patrick after Orlando 99
4-DTC2	211		4-TC1	Hoyt after Orlando 99
4-DTC3	233, 235		4-TC2	
4-DTC4	234, 248		4-TC2	
4-DTC5	228, 242, 265	10 Jan 2001	4-TC2	Erik after Orlando 2001
ITU-T Rec. X.519 (1997) | ISO/IEC 9594-5:1998				
5-DTC1	221		5-TC1	Ella after Orlando 99
5-DTC2	236		5-TC2	
5-DTC3	228, 242, 266	10 Jan 2001	5-TC2	Erik after Orlando 2000
ITU-T Rec. X.520 (1997) | ISO/IEC 9594-6:1998				
6-DTC1	211		6-TC1	Hoyt after Orlando 99
6-DTC2	237, 238, 241		6-TC2	
6-DTC3	270	10 Jan 2001	6-TC2	Erik after Orlando 2001
ITU-T Rec. X.521 (1997) | ISO/IEC 9594-7:1998				
7-DTC1	239		7-TC1	

DTC #	Defect Reports resolved	Ballot Close	Published As	History
ITU-T Rec. X.509 (1997) I ISO/IEC 9594-8:1998				
8-DTC1	183, 194		3rd edition	Incorporated into published edition
8-DTC3	200, 201, 212, 213, 218, 220		8-TC1	Sharon after Orlando 99
8-DTC4	185		8-TC1	Sharon after Orlando 99
8-DTC5	204		8-TC1	Sharon after Orlando 99
8-DTC7	222		8-TC1	Sharon after Orlando 99
8-DTC8	226, 227, 240		8-TC? *in preparation*	
8-DTC9	244, 256, 257, 258		8-TC? *in preparation*	Sharon after Orlando 2000, comments resolved at Geneva 2001
ITU-T Rec. X.525 (1997) I ISO/IEC 9594-9:1998				
9-DTC1	182, 186		9-TC1	Processed at Helsinki 97 and produced by Hoyt after Orlando 99
9-DTC2	187, 208, 243		9-TC2	
9-DTC3	245		9-TC2	
9-DTC4	228, 242	10 Jan 2001	9-TC2	Erik after Orlando 2001
ITU-T Rec. X.530 (1997) I ISO/IEC 9594-10:1998				
10-DTC1	252	10 Jan 2001	10-TC1	Erik after Orlando 2001

Recommendation X.501 (1997) | ISO/IEC 9594-2:1998

Information processing systems - Open Systems Interconnection - The Directory - Models

TECHNICAL CORRIGENDUM 1

NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 1 and 2.

Defect reports resolved by Draft Technical Corrigendum 1
(defect reports 173, 179, 189,)

This corrects the defects reported in defect report 9594/173.

Clause 20.5 First Level DSAs

Change the text of bullet c) the following way:

d) It holds subordinate references (of category master and/or shadow) and non-specific subordinate references (of category master and/or shadow) which account for all the naming contexts immediately subordinate to the root of the DIT which it does not itself hold.

This corrects the defects reported in defect report 9594/179.

Annex J, Table J-1

In the second column called "Entry protected Item Permissions Required", add the following texts for the Read and the Search operations:

For the Read operation:

"*ReturnDN* for distinguished name"

For the Search Operation:

"*ReturnDN* for each returned distinguished name"

This corrects the defects reported in defect report 9594/189.

Clause 26.3 Modify Operational Binding
and **Annex F**

Add OPTIONAL to the ASN.1 of **newAgreement** *:*

```
newAgreement    [7]      OPERATIONAL-BINDING.&Agreement
                         ({OpBindingSet}{@bindingType}) OPTIONAL,
```

This corrects the defects reported in defect report 9594/205.

Clause 20.3.2. Knowledge Reference Types

Change the first bullet point after "A DSA may hold the following types of knowledge reference:" *to read:*

- superior references;

Clause 20.3.2.1. Superior Reference

Change the title and second sentence to read:

20.3.2.1 Superior References

A superior reference consists of

– the Access Point of a DSA.

Each non-first level DSA (see 20.5) shall maintain at least one superior reference.

Clause 20.4.1. Superior Knowledge

Change the first sentence to read:

Each DSA that is not a first level DSA shall maintain at least one superior reference.

And add the following second sentence:

Additional superior references may be held for operational reasons as alternative paths to the root of the DIT.

Clause 20.5. First Level DSAs

Change the second sentence to read:

“A DSA referenced by other DSAs may itself maintain one or more superior references.”

Change the last sentence to read:

“They therefore may serve as a superior reference for non-first level DSAs.”

Clause21.4.2. DSE Types h)

Change it to read:

h) **supr**: A DSE that holds a specific knowledge attribute to represent the DSAs superior references.

Clause 22.2.1.2. Superior Knowledge

Change the first sentence to plural and the ATTRIBUTE SYNTAX to SET OF, to read:

The **superiorKnowledge** operational attribute type is used by a non-first level DSA to represent its superior references.

```
superiorKnowledge       ATTRIBUTE           ::=     {WITH SYNTAX        SET OF
                        AccessPoint
                        .....
```

Clause 22.2.2.2. Superior Reference

Insert a new second sentence:

Since a **superiorKnowledge** attribute value may contain the access points of several DSAs, it may therefore represent several superior references.

Defect reports resolved by Draft Technical Corrigendum 2

(defect report 211)

This corrects the defects reported in defect report 9594/211.

Clause 26.2

Change the two occurrences of **UTCTime** *to* **Time***:*

Insert the following after the ASN.1 definition of **Validity**

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

Before a value of **Time** is used in any comparison operation and if the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Clause 26.4

Change **UTCTime** *to* ***Time****:*

Clause 26.5

Change **UTCTime** *to* ***Time****:*

Also make theASN.1 changes to Annex F.

Recommendation X.501 (1997) | ISO/IEC 9594-2:1998 Technical Corrigendum 2

NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 3 and 4.

Defect reports resolved by Draft Technical Corrigendum 3

(defect reports 229 and 230)

This corrects the defects reported in defect reports 9594/229-230.

In 2.1:

Replace:

– ITU-T Recommendation X.525 (1997) | ISO/IEC 9594-8:1999, *Information technology – Open Systems Interconnection – The Directory: Replication*.

with:

– ITU-T Recommendation X.525 (1997) | ISO/IEC 9594-9:1998, *Information technology – Open Systems Interconnection – The Directory: Replication*.

In 17.4.3:

In the **attributeValueSecurityLabelContext** specification replace **SYNTAX** with **WITH SYNTAX**

Delete the **KeyIdentifier** type.

The same changes shall be done in Annex P

In 18.1.2:

Change the 4th paragraph to:

Digital signatures applied to the whole entry do not include operational, ~~or~~ collective attributes or the **attributeIntegrityInfo** itself. Any attribute value contexts are included.

Delete the 5th paragraph (Additional control information …).

Change the **attributeIntegrityInfo** *attribute definition and its supporting definitions to:*

```
attributeIntegrityInfo ATTRIBUTE  ::= {
        WITH SYNTAX                         AttributeIntegrityInfo
        ID                                  id-at-attributeIntegrityInfo}

AttributeIntegrityInfo  ::=  SIGNED { 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 { SEQUENCE SIZE (1..MAX) OF Attribute }
                -- Attribute type and values with associated context values for the selected Scope
```

Add the following text after the above ASN.1:

An **AttributeIntegrityInfo** value can be created in three different ways:

a) An administrative authority can create and sign the value, and the public key to verify the signature is known by off-line means.

b) The owner of the entry, i.e. the object represented by the entry, can create and sign the value. If the owner has several certificates, or expected to have that in the future, the certificate has to be identified by the CA issuing the certificate together with the certificate serial number.

c) A third party may create and sign the value. The name of the signer, the name of the CA issuing the certificate and the certificate serial number is required.

If the scope is **wholeEntry**, all the applicable attributes shall be ordered as specified for a set-of type in 6.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8. If scope is **selectedTypes**, the ordering shall be the same as the one given in the **SelectedTypes**.

NOTE – If a user does not retrieve all the complete attributes that are defined within the **Scope** data type, it will not be possible for the user to verify the integrity of the attributes.

Delete 18.1.2.1.

The changes to ASN.1 shall also be done in Annex P.

Replace 18.1.3 with:

18.1.3 Context for Protection of a Single Attribute Value

The following defines a context to hold a digital signature, along with associated control information, which provides integrity for a single attribute value. Any attribute value contexts are included in the integrity check, excluding the context used to hold signatures.

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

AttributeValueIntegrityInfo  ::=  SIGNED { 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 }
```

The **contextList** shall be ordered as specified for a set-of type in 6.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8.

Change the ASN.1 ASN.1 in Annex P as per above and delete ***AVIAssertion*** *data type.*

In annex B:

Delete **OPTIONALLY-SIGNED** import from **DirectoryAbstractService**

In annex C:

In the **application** component of **AttributeTypeInformation** replace **userApplication** with **userApplications**

In Annex D:

Add **directoryAbstractService** to the import from **UsefulDefinitions**
Add **SupportedAttributes** to the import from **InformationFramework**
Add:

```
Filter
   FROM DirectoryAbstractService directoryAbstractService
```

In annex F:

Add **enhancedSecurity** to the import from **UsefulDefinitions**
Delete **OPTIONALLY-PROTECTED** and **DIRQOP** from the import from **EnhancedSecurity**. Add instead **OPTIONALLY-PROTECTED-SEQ**.

In annex P:

All the changes to annex P has been subsumed by the resolution of defect report 228

Defect reports resolved by Draft Technical Corrigendum 4

(defect reports 228, 242, 255, 260, 261, 267 and 269)

This corrects the defects reported in defect report 9594/228.

Add at the beginning of 15.3 just before 15.3.1:

Warning – Subclause 15.3.1 and 15.3.2 are known to contain invalid specifications. These subclauses are therefore deprecated. A future edition will either remove the deprecated specifications or provide updated text.

The following specifications are provided to preserve the optionally signed capability provided by edition 2 of these Directory Specifications and to allow that capability to be extended to all operations and to errors:

OPTIONALLY-PROTECTED is a parameterized data type where the parameter is a data type whose values may, at the option of the generator, be accompanied by their digital signature. This capability is specified by means of the following type:

```
OPTIONALLY-PROTECTED { Type }  ::=  CHOICE {
      unsigned            Type,
      signed        SIGNED {Type} }
```

The **OPTIONALLY-PROTECTED-SEQ** is used instead of **OPTIONALLY-PROTECTED** when the protected data type is a sequence data type that is not tagged.

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

The **SIGNED** parameterized data type, which describes the form of the signed form of the information, is specified in ITU-T Rec. X.509 | ISO/IEC 9594-8.

Add at the beginning of 18.2 just before 18.2.1:

Warning – This subclause is known to contain invalid specifications. This subclause is therefore deprecated. A future edition will either remove the deprecated specifications or provide updated text.

In Annex A, add ASN.1 comment item as shown:

```
-- securityExchange                ID    ::=    {ds 32}

-- directorySecurityExchanges      ID    ::=    {module directorySecurityExchanges (29) 4}

-- id-se                           ID    ::=    securityExchange
```

In clause 26, delete any occurrence of

,

```
        DIRQOP.&...-QOP{@dirqop}
```

and change all occurrences of:

```
        OPTIONALLY-PROTECTED
```

to:

```
        OPTIONALLY-PROTECTED-SEQ
```

The same changes shall be made to Annex F.

Replace Annex P with:

Annex P

Enhanced security

(This annex forms an integral part of this Recommendation | International Standard)

This module is known to contain invalid specifications. Part of this module is therefore deprecated. The deprecated part is indicated by ASN.1 comment items. A future edition will either remove the deprecated specifications or provide updated specifications.

```
EnhancedSecurity { joint-iso-itu-t ds(5) modules(1) enhancedSecurity(28) 4 }
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,
        informationFramework, upperBounds
                FROM UsefulDefinitions { joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 4 }

        Attribute, ATTRIBUTE, AttributeType, Context, CONTEXT, MATCHING-RULE, Name,
        objectIdentifierMatch, SupportedAttributes
                FROM InformationFramework informationFramework

        AttributeTypeAndValue
                    FROM BasicAccessControl basicAccessControl

-- from ITU-T Rec. X.509 | ISO/IEC 9594-8

        AlgorithmIdentifier, CertificateSerialNumber, ENCRYPTED{}, HASH{}, SIGNED{}
                    FROM AuthenticationFramework authenticationFramework

        GeneralName, KeyIdentifier
                    FROM CertificateExtensions certificateExtensions

        ub-privacy-mark-length
                FROM UpperBounds upperBounds  ;
-- from GULS
-- SECURITY-TRANSFORMATION, PROTECTION-MAPPING, PROTECTED
--          FROM Notation { joint-iso-ccitt genericULS (20) modules (1) notation (1) }

--dirSignedTransformation, KEY-INFORMATION
--          FROM GulsSecurityTransformations { joint-iso-ccitt genericULS (20) modules (1)
--                gulsSecurityTransformations (3) }

-- signed
--          FROM GulsSecurityTransformations { joint-iso-ccitt genericULS (20) modules (1)
--                dirProtectionMappings (4) };

-- The "signed" Protection Mapping and associated "dirSignedTransformations" imported
-- from the Generic Upper Layers Security specification (ITU-T Rec. X.830 | ISO/IEC 11586-1)
-- results in identical encoding as the same data type used with the SIGNED as defined in
-- ITU-T REC. X.509 | ISO/IEC 9594-8
-- The three statements below are provided temporarily to allow signed operations to be supported as in
edition 3.

OPTIONALLY-PROTECTED { Type }  ::=  CHOICE {
        unsigned              Type,
        signed        SIGNED {Type} }

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

-- The following out-commented ASN.1 specification are know to be erroneous and are therefore
deprecated.

-- genEncryptedTransform {KEY-INFORMATION: SupportedKIClasses }  SECURITY-
TRANSFORMATION  ::=
--      {
--      IDENTIFIER                          { enhancedSecurity  gen-encrypted(2) }
--      INITIAL-ENCODING-RULES              { joint-iso-itu-t  asn1(1)  ber(1) }
                                       -- This default for initial encoding rules may be overridden
                                       -- using a static protected parameter (initEncRules).
--          XFORMED-DATA-TYPE                 SEQUENCE {
--                    initEncRules   OBJECT IDENTIFIER DEFAULT { joint-iso-itu-t  asn1(1)  ber(1) },
--                    encAlgorithm  AlgorithmIdentifier OPTIONAL, --  -- Identifies the encryption
algorithm,
--                    keyInformation            SEQUENCE {
--                          kiClass    KEY-INFORMATION.&kiClass ({SupportedKIClasses}),
--                          keyInfo    KEY-INFORMATION.&KiType ({SupportedKIClasses} {@kiClass})
--                                     } OPTIONAL,
                            -- Key information may assume various formats, governed by supported
members
                            -- of the KEY-INFORMATION information object class (defined in ITU-T
                            -- Rec. X.830 | ISO/IEC 11586-1)
--                    encData          BIT STRING ( CONSTRAINED BY {
                            -- the encData value must be generated following
                            -- the procedure specified in 17.3.1-- -- })
--                    }
--          }

-- encrypted  PROTECTION-MAPPING  ::=  {
--          SECURITY-TRANSFORMATION { genEncryptedTransform } }

-- signedAndEncrypt  PROTECTION-MAPPING  ::=  {
--          SECURITY-TRANSFORMATION  { signedAndEncryptedTransform } }

-- signedAndEncryptedTransform {KEY-INFORMATION: SupportedKIClasses}
--      SECURITY-TRANSFORMATION  ::=  {
--            IDENTIFIER                { enhancedSecurity  dir-encrypt-sign (1) }
--            INITIAL-ENCODING-RULES { joint-iso-itu-t asn1 (1) ber-derived (2) distinguished-
encoding (1) }
--            XFORMED-DATA-TYPE
--              PROTECTED
--              {
--                    PROTECTED
--                    {
--                    ABSTRACT-SYNTAX.&Type,
--                    signed
--                    },
--              encrypted
--              }
--      }

-- OPTIONALLY-PROTECTED {ToBeProtected, PROTECTION-MAPPING:generalProtection} ::=
--          CHOICE {
--              toBeProtected        ToBeProtected,
                                       --no DIRQOP specified for operation
--              signed      PROTECTED {ToBeProtected, signed},
                                       --DIRQOP is Signed
--              protected              [APPLICATION 0]
--                                     PROTECTED { ToBeProtected, generalProtection } }
                                       --DIRQOP is other than Signed
```

```
-- defaultDirQop ATTRIBUTE  ::=  {
--        WITH SYNTAX                              OBJECT IDENTIFIER
--        EQUALITY MATCHING RULE        objectIdentifierMatch
--        USAGE                                    directoryOperation
--        ID                                       id-at-defaultDirQop }

-- DIRQOP  ::=  CLASS
-- This information object class is used to define the quality of protection
-- required throughout directory operation.
-- The Quality Of Protection can be signed, encrypted, signedAndEncrypt
-- {
--        &dirqop-Id                                             OBJECT IDENTIFIER UNIQUE,
--        &dirBindError-QOP                                      PROTECTION-
MAPPING:protectionReqd,
--        &dirErrors-QOP                                         PROTECTION-
MAPPING:protectionReqd,
--        &dapReadArg-QOP                                        PROTECTION-
MAPPING:protectionReqd,
--        &dapReadRes-QOP                                        PROTECTION-
MAPPING:protectionReqd,
--        &dapCompareArg-QOP                             PROTECTION-
MAPPING:protectionReqd,
--        &dapCompareRes-QOP                             PROTECTION-
MAPPING:protectionReqd,
--        &dapListArg-QOP                                PROTECTION-
MAPPING:protectionReqd,
--        &dapListRes-QOP                                PROTECTION-
MAPPING:protectionReqd,
--        &dapSearchArg-QOP                                      PROTECTION-
MAPPING:protectionReqd,
--        &dapSearchRes-QOP                                      PROTECTION-
MAPPING:protectionReqd,
--        &dapAbandonArg-QOP                             PROTECTION-
MAPPING:protectionReqd,
--        &dapAbandonRes-QOP                             PROTECTION-
MAPPING:protectionReqd,
--        &dapAddEntryArg-QOP                            PROTECTION-
MAPPING:protectionReqd,
--        &dapAddEntryRes-QOP                            PROTECTION-
MAPPING:protectionReqd,
--        &dapRemoveEntryArg-QOP                                 PROTECTION-
MAPPING:protectionReqd,
--        &dapRemoveEntryRes-QOP                                 PROTECTION-
MAPPING:protectionReqd,
--        &dapModifyEntryArg-QOP                         PROTECTION-
MAPPING:protectionReqd,
--        &dapModifyEntryRes-QOP                         PROTECTION-
MAPPING:protectionReqd,
--        &dapModifyDNArg-QOP                            PROTECTION-
MAPPING:protectionReqd,
--        &dapModifyDNRes-QOP                            PROTECTION-
MAPPING:protectionReqd,
--        &dspChainedOp-QOP                                      PROTECTION-
MAPPING:protectionReqd,
--        &dispShadowAgreeInfo-QOP                       PROTECTION-
MAPPING:protectionReqd,
--        &dispCoorShadowArg-QOP                                 PROTECTION-
MAPPING:protectionReqd,
--        &dispCoorShadowRes-QOP                                 PROTECTION-
MAPPING:protectionReqd,
--        &dispUpdateShadowArg-QOP                       PROTECTION-
MAPPING:protectionReqd,
--        &dispUpdateShadowRes-QOP                       PROTECTION-
MAPPING:protectionReqd,
--        &dispRequestShadowUpdateArg-QOP                PROTECTION-
MAPPING:protectionReqd,
--        &dispRequestShadowUpdateRes-QOP                PROTECTION-
MAPPING:protectionReqd,
--        &dopEstablishOpBindArg-QOP                     PROTECTION-
MAPPING:protectionReqd,
--      &dopEstablishOpBindRes-QOP                          PROTECTION-
MAPPING:protectionReqd,
--      &dopModifyOpBindArg-QOP                             PROTECTION-
MAPPING:protectionReqd,
--      &dopModifyOpBindRes-QOP                             PROTECTION-
MAPPING:protectionReqd,
--      &dopTermOpBindArg-QOP                               PROTECTION-
MAPPING:protectionReqd,
--      &dopTermOpBindRes-QOP                                   PROTECTION-
MAPPING:protectionReqd
-- }
-- WITH SYNTAX
-- {
--      DIRQOP-ID                                               &dirqop-Id
--      DIRECTORYBINDERROR-QOP                              &dirBindError-QOP
--      DIRERRORS-QOP                                       &dirErrors-QOP
--      DAPREADARG-QOP                                          &dapReadArg-QOP
--      DAPREADRES-QOP                                          &dapReadRes-QOP
--      DAPCOMPAREARG-QOP                                   &dapCompareArg-QOP
--      DAPCOMPARERES-QOP                                   &dapCompareRes-QOP
--      DAPLISTARG-QOP                                      &dapListArg-QOP
--      DAPLISTRES-QOP                                      &dapListRes-QOP
--      DAPSEARCHARG-QOP                                    &dapSearchArg-QOP
--      DAPSEARCHRES-QOP                                    &dapSearchRes-QOP
--      DAPABANDONARG-QOP                                   &dapAbandonArg-QOP
--      DAPABANDONRES-QOP                                   &dapAbandonRes-QOP
--      DAPADDENTRYARG-QOP                                  &dapAddEntryArg-QOP
--      DAPADDENTRYRES-QOP                                  &dapAddEntryRes-QOP
--      DAPREMOVEENTRYARG-QOP                               &dapRemoveEntryArg-QOP
--      DAPREMOVEENTRYRES-QOP                               &dapRemoveEntryRes-QOP
--      DAPMODIFYENTRYARG-QOP                               &dapModifyEntryArg-QOP
--      DAPMODIFYENTRYRES-QOP                               &dapModifyEntryRes-QOP
--      DAPMODIFYDNARG-QOP                                  &dapModifyDNArg-QOP
--      DAPMODIFYDNRES-QOP                                  &dapModifyDNRes-QOP
--      DSPCHAINEDOP-QOP                                        &dspChainedOp-QOP
--      DISPSHADOWAGREEINFO-QOP                             &dispShadowAgreeInfo-QOP
--      DISPCOORSHADOWARG-QOP                               &dispCoorShadowArg-QOP
--      DISPCOORSHADOWRES-QOP                               &dispCoorShadowRes-QOP
--      DISPUPDATESHADOWARG-QOP                             &dispUpdateShadowArg-QOP
--      DISPUPDATESHADOWRES-QOP                             &dispUpdateShadowRes-QOP
--      DISPREQUESTSHADOWUPDATEARG-QOP                      &dispRequestShadowUpdateArg-QOP
--      DISPREQUESTSHADOWUPDATERES-QOP                      &dispRequestShadowUpdateRes-
QOP
--      DOPESTABLISHOPBINDARG-QOP                           &dopEstablishOpBindArg-QOP
--      DOPESTABLISHOPBINDRES-QOP                           &dopEstablishOpBindRes-QOP
--      DOPMODIFYOPBINDARG-QOP                              &dopModifyOpBindArg-QOP
--      DOPMODIFYOPBINDRES-QOP                              &dopModifyOpBindRes-QOP
--      DOPTERMINATEOPBINDARG-QOP                           &dopTermOpBindArg-QOP
--      DOPTERMINATEOPBINDRES-QOP                           &dopTermOpBindRes-QOP
-- }

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

SignedSecurityLabel  ::=  SIGNED {SEQUENCE  {
        attHash         HASH {AttributeTypeAndValue},
        issuer          Name                    OPTIONAL,  -- name of labelling authority
        keyIdentifierKeyIdentifier   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 presen-- } ) )

SecurityPolicyIdentifier  ::=  OBJECT IDENTIFIER
```

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

PrivacyMark  ::=  PrintableString (SIZE (1..ub-privacy-mark-length))

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
        ID                                  id-at-attributeIntegrityInfo }

AttributeIntegrityInfo  ::=  SIGNED { 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,
        specificIssuerAndSerialNumber }

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 { SEQUENCE SIZE (1..MAX) OF Attribute }
                    -- Attribute type and values with associated context values for the selected Scope

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

AttributeValueIntegrityInfo  ::=  SIGNED { 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 }

-- The following out-commented ASN.1 specification are know to be erroneous and are therefore
deprecated.

-- EncryptedAttributeSyntax {AttributeSyntax}  ::=  SEQUENCE  {
--      keyInfo SEQUENCE OF KeyIdOrProtectedKey,
--      encAlg  AlgorithmIdentifier,
--      encValue     ENCRYPTED { AttributeSyntax } }

-- KeyIdOrProtectedKey  ::=  SEQUENCE  {
--      keyIdentifier[0]      KeyIdentifier   OPTIONAL,
--      protectedKeys        [1]        ProtectedKey  OPTIONAL }
                 -- At least one key identifier or protected key must be present

-- ProtectedKey  ::=  SEQUENCE  {
--      authReaders          AuthReaders,--           -- if absent, use attribute in authorized reader entry
--      keyEncAlg   AlgorithmIdentifier  OPTIONAL, --           --  algorithm to encrypt encAttrKey
--      encAttKey            EncAttKey  }
                                -- confidentiality key protected with authorized user's
                                -- protection mechanism

-- AuthReaders  ::=  SEQUENCE OF Name

-- EncAttKey  ::=  PROTECTED {SymmetricKey, keyProtection}

-- SymmetricKey  ::=  BIT STRING

-- keyProtection PROTECTION-MAPPING  ::=  {
--      SECURITY-TRANSFORMATION {genEncryption} }

-- confKeyInfo  ATTRIBUTE  ::=  {
--      WITH SYNTAX                           ConfKeyInfo
--      EQUALITY MATCHING RULE       readerAndKeyIDMatch
--      ID                           id-at-confKeyInfo }

-- ConfKeyInfo  ::=  SEQUENCE  {
--      keyIdentifierKeyIdentifier,
--      protectedKey         ProtectedKey }

-- readerAndKeyIDMatch MATCHING-RULE  ::=  {
--      SYNTAX      ReaderAndKeyIDAssertion
--      ID        id-mr-readerAndKeyIDMatch }

-- ReaderAndKeyIDAssertion  ::=  SEQUENCE {
--      keyIdentifierKeyIdentifier,
--      authReaders          AuthReaders OPTIONAL }
-- Object identifier assignments --
-- 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
```

This corrects the defects reported in defect report 9594/242.
Add size limit **SIZE (1..MAX)** to all optional **SET OF** and **SEQUENCE OF** constructs.

This corrects the defects reported in defect reports 9594/255.

In 12.7.2 and in Annex A, change in the ***CONTENT-RULE*** *information object class from:*

```
        &structuralClass                OBJECT-CLASS.&id  UNIQUE,
```

to:

```
        &structuralClass                OBJECT-CLASS              UNIQUE,
```

This corrects the defects reported in defect reports 9594/260.

Update the ***AttributeTypeAndDistinguishedValue*** *as shown:*

```
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 }
```

This corrects the defects reported in defect reports 9594/261.
Replace **CommonResults** with **CommonResultsSeq** in all ASN.1 constructs and in the import in Annex F.
In last paragraph of 26.5 (28.5 in addition 4) replace **CommonResults** with **CommonResultsSeq**.

This corrects the defects reported in defect reports 9594/267.
In NOTE 1 of 14.7.3, replace ITU-T Rec. X.680 | ISO/IEC 8824-1 with ITU-T Rec. X.682 | ISO/IEC 8824-3
Replace NOTE 1 in 14.7.10 with a copy of NOTE 1 in 14.7.3, but keep the last sentence.
In 25.2, swap Figure 19 and 20, but not the figure text.
In 22.2.1.2, make the **superiorKnowledge** attribute multi-valued and return to the old syntax (**AccessPoint**).

This corrects the defects reported in defect reports 9594/269.

In 12.5.2, item a), replace:

rule is applied to;

with:

...rule is applied to unless the matching rule specifies otherwise;

In 14.7.3 add **OPTIONAL** *to the* ***information*** *component of* ***MatchingRuleDescription***

Recommendation X.511 (1997) | ISO/IEC 9594-3:1998

Information processing systems - Open Systems Interconnection - The Directory - Abstract Service Definition

TECHNICAL CORRIGENDUM 1
NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 1 and 2.

Defect reports resolved by Draft Technical Corrigendum 1

(defect reports 166, 179, 188, 202, 206, 217)

This corrects the defects reported in defect report 9594/166.

Clause 7.11.1.1 Alias derefencing

Change the second last sentence of first paragraph of 7.11.1.1 the following way:

If the DSA chains the request to another DSA and receives back a referral from it, then the access controls shall be applied to the referral if the targetObject in the referral is the same as in the chained request.

This corrects the defects reported in defect report 9594/179.

Annex B, Figure B-4

In the flow chart "return of DN" add under the question "alias name available?/No" an additional question :

"Read operation?"

with the following outputs :

Yes : Name Error
No : *go to next question : "entry corresponds to (base) object of DAP operation?*

Annex B, Figure B-5

In the flow chart "Read Operation" change on the right part the text of the last step of handling "selection empty = yes"
from "return Read result" *to* "return Read result or nameError" .

This corrects the defects reported in defect report 9594/188.

Clause 11.1.5 Add operation decision points for basic-access-control, bullet 3) , note 2

Reword the note 2 to read:

“The Add permission must be provided as prescriptiveACI when attempting to add an entry and as prescriptiveACI or subentryACI when attempting to add a subentry.”

This corrects the defects reported in defect report 9594/202.

Clause 7.10 Security Parameters

Replace the paragraph describing **CertificationPath** *with the following*

The **CertificationPath** component is a sequence containing the signer’s user certificate, and, optionally, a sequence of one or more certification authority (CA) certificates. (See clause 8 in ITU-T Rec. X.509 | ISO/IEC 9594-8). The user certificate is used to bind the signer's public key and distinguished name, and may be used to verify the signature on a request argument, response, or error. This parameter shall be present and contain the signer’s user certificate if the request argument, response, or error is signed. Additional certificates may be present and may be used to determine if the signer’s user certificate is valid. Additional certificates are not required if the recipient shares the same certification authority as the signer. If the recipient requires a certification path for validation, and an acceptable parameter is not present, whether the recipient rejects the signature, or attempts to determine a certification path, is a local matter.

Replace the paragraph describing **time** *with the following*

The **time** is the intended expiry time for the validity of the request, response, or error. It is used in conjunction with the random number to enable the detection of replay attacks.

Replace the 1st paragraph describing **random** *with the following*

The **random** value is a number that should be different for each request, response, or error. It is used in conjunction with the time parameter to enable the detection of replay attacks. If sequence integrity is required then the random argument may be used to carry a sequence integrity number as follows: …

Defect reports resolved by Draft Technical Corrigendum 2

(covering resolution to defect report 211)

This corrects the defects reported in defect report 9594/206.

Clause 10.1.3 List results

In the second last paragraph of the clause, change the first part of the first sentence (“When a DUA has requested a protection request of signed, the uncorrelatedListInfo prameter…”) the following way :

“When the DUA has requested a protection request of signed, or if the Directory for other reasons are not able to correlate information, the **uncorrelatedListInfo** parameter...”

This corrects the defects reported in defect report 9594/217.

Clause 7.10 Security parameters

a) Replace syntax for operationCode in SecurityParameters to be:

```
operationCode [6] Code OPTIONAL
```

Code *should be imported from:*
Remote-Operations-Information-Objects
{joint-iso-ccitt remote-operations(4) informationObjects(5) version1(0)}

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

b) Add to the SecurityParameters syntax:

```
errorCode        [9]       Code OPTIONAL
```

and add the following description:

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

(defect reports 211)

This corrects the defects reported in defect report 9594/211.

Clause 7.10

Change **UTCTime** *to* **Time***:*

Insert the following after the ASN.1 definition of **ProtectionRequest**

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

Insert the following after the last paragraph of 7.10 .

If the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

- If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — **GeneralizedTime** shall be used if the negotiated version is **v2** or greater. The use of **GeneralizedTime** when **v1** has been negotiated may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Clause 8.1.1

Change the value of **validity** *in the ASN.1 type* **SimpleCredentials** *to*

```
validity    [1]        SET {
        validityPeriod         CHOICE  {
                   COMPONENTS OF ValidityPeriodUTC,  -- UTC when v1
                   COMPONENTS OF ValidityPeriodGT },  -- GT when > v1
        random1    [2]         BIT STRING  OPTIONAL,
        random2    [3]         BIT STRING  OPTIONAL} OPTIONAL,
```

Insert the following after the ASN.1 type **SimpleCredentials** *to*

```
ValidityPeriodUTC              ::=        SET {
        time1         [0]      UTCTime OPTIONAL,
        time2         [1]      UTCTime OPTIONAL }
ValidityPeriodGT  ::=          SET {
        time1         [0]      GeneralizedTime OPTIONAL,
        time2         [1]      GeneralizedTime OPTIONAL }
```

Clause 8.1.2

Insert the following after the second paragraph.

Note — **ValidityPeriodGT** shall be used if the negotiated version is **v2** or greater. The use of **ValidityPeriodGT** when **v1** has been negotiated may prevent interworking with implementations unaware of the possibility of choosing either **ValidityPeriodUTC** or **ValidityPeriodGT**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **ValidityPeriodGT** may be used. In no case shall **ValidityPeriodUTC** be used for representing dates beyond 2049.

Change the value of **time** *in the ASN.1 type* **Token** *to*

```
        time          [2]      Time,
```

Also make theASN.1 changes to Annex A.

Recommendation X.511 (1997) | ISO/IEC 9594-3:1998
Technical Corrigendum 2

NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 3, 4, and 5.

Defect reports resolved by Draft Technical Corrigendum 3

(defect reports 231 and 232)

This corrects the defects reported in defect report 9594/231.

This technical corrigendum makes modifications to technical corrigendum 2.

Instead of the ASN.1 suggested in corrigendum 2, use the following data type:

```
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 },
        password               [2]       CHOICE {
                unprotected                       OCTET STRING,
                protected                                    SIGNATURE {OCTET STRING} } OPTIONAL}
```

Change the notes suggested for 7.10 and 8.1.1 to normative text.

This corrects the defects reported in defect report 9594/232.

General:

Change all occurrences of **joint-iso-ccitt** to **joint-iso-itu-t**

In "7.2 Information types defined elsewhere":

Replace **OPTIONALLY-SIGNED** with **OPTIONALLY-PROTECTED** and **OPTIONALLY-PROTECTED-SEQ**

In annex A:

add **basicAccessControl** and **enhancedSecurity** to the import from **UsefulDefinitions**

Add a new import:

```
AttributeTypeAndValue
   FROM BasicAccessControl  basicAccessControl
```

Add **ENCRYPTED** to the import from **AuthenticationFramework**

Move the semicolon from the end of the import from **Remote-Operations-Generic-ROS-PDUs** to the end of import from **SpkmGssTokens**.

In the import from **SpkmGssTokens**, change **SPKM-REP-IT** to **SPKM-REP-TI**

Defect reports resolved by Draft Technical Corrigendum 4

(defect reports 247)

This corrects the defects reported in defect report 9594/247.

In the Introduction, change from:

Annex B, which is an integral part of this Recommendation | International Standard, ..

to:

Annex B, which is not an integral part of this Recommendation | International Standard, ..

In 7.4, add the following construct and explanatory note after **CommonResults**:

```
CommonResultsSeq  ::=  SEQUENCE {
        securityParameters          [30]    SecurityParameters                  OPTIONAL,
        performer                   [29]    DistinguishedName                   OPTIONAL,
        aliasDereferenced  [28]     BOOLEAN
        DEFAULT FALSE }
```

NOTE – **CommonResults** and **CommonResultsSeq** consist of the same components. The former is used when included in set types by the **COMPONENT OF** type, while the latter is used similarly in sequenced types.

In the **AbandonResult**, **AddEntryResult**, **RemoveEntryResult**, **ModifyEntryResult** and **ModifyDNResult** change **CommonResults** to **CommonResultsSeq**

Defect reports resolved by Draft Technical Corrigendum 5

(defect reports 224, 228, 242, and 263)

This corrects the defects reported in defect report 9594/224.

In subclause 7.8, change "undefined" *to* "UNDEFINED" *in all places to indicate parity with "TRUE" and "FALSE" for the three-valued logic defined in this subclause.*

In subclause 7.8.2, add to the end of 3rd paragraph:

> When these conditions are not met, the **FilterItem** shall evaluate to the logical value UNDEFINED.

Delete NOTE 1 and change NOTE 2 (which is now NOTE 1) to:

NOTE 1 – Access control restrictions may affect the evaluation of the **FilterItem** and may cause the **FilterItem** to evaluate to UNDEFINED.

Insert new paragraph after the new NOTE 1:

> An assertion which is defined by these conditions additionally evaluates to UNDEFINED if it relates to an attribute value and the attribute type is not present in an attribute against which the assertion is being tested. An assertion which is defined by these conditions and relates to the presence of an attribute type evaluates to FALSE.

This corrects the defects reported in defect report 9594/228.

Delete any occurrence of

```
                                                          ,
        DIRQOP.&…-QOP{@dirqop}
```

In 9.3, change **OPTIONALLY-PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ** *in both* ***AbandonArgument*** *and* ***AbandonResult***.

In 11.1.1, change **PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ** *in* ***AddEntryResult***.

In 12.1.1, change **PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ** *in* ***RemoveEntryResult***.

In 13.1.1, change **OPTIONALLY-PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ** *in* ***ModifyEntryResult***.

In 14.1.1, change **OPTIONALLY-PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ** *in* ***ModifyDNResult***.

In Annex A, make the changes as indicated above.

In Annex A, delete

```
        PROTECTED
                FROM Notation { joint-iso-itu-t genericULS (20) modules (1) notation (1) }
```

In Annex A, add **OPTIONALLY-PROTECTED-SEQ** *to and delete* **DIRQOP** *from the import from* ***EnhancedSecurity***.

This corrects the defects reported in defect report 9594/242.

Add size limit **SIZE (1..MAX)** to all optional **SET OF** and **SEQUENCE OF** constructs.

This corrects the defects reported in defect report 9594/263.
Change the last sentence of the second to the paragraph of 7.1 to:

> Each of the subclauses 7.3 through 7.10 identifies and defines an information type.

Delete NOTE 1 in 8.1.2.

Change the third paragraph of 8.1.2 to:

> **GeneralizedTime** shall be used for **time1** and **time2** if the negotiated version is **v2** or greater. The use of **GeneralizedTime** when **v1** has been negotiated may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime.** It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. **UTCTime** shall not be used for representing dates beyond 2049.

Recommendation X.518 (1997) I ISO/IEC 9594-4:1998

Information processing systems - Open Systems Interconnection - The Directory - Procedures for Distributed Operation

TECHNICAL CORRIGENDUM 1
NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 1 and 2.

Defect reports resolved by Draft Technical Corrigendum 1
(defect reports 157, 159, 162, 180, 190, 198, 206, 209)

This corrects the defects reported in defect report 9594/157.

Clause 19.1.4 Modify DN operation

After the first paragraph of bullet 9), add the new paragraph:

"If the entry, alias entry or subentry was within the UnitOfReplication of one or more shadowing agreements held by the DSA, and the superior of the renamed entry, alias entry or subentry is not within this UnitOfReplication, the shadow consumers shall be updated using the procedures of the Directory shadow service specified in ITU-T Rec. X.525|ISO/IEC 9594-9; in this case the shadowed entry and all its subordinates shall be removed.

If the entry, alias entry or subentry was not within the UnitOfReplication of one or more shadowing agreements held by the DSA, and the renamed entry, alias entry or subentry is now within this UnitOfReplication, the shadow consumers shall be updated using the procedures of the Directory shadow service specified in ITU-T Rec. X.525|ISO/IEC 9594-9; in this case the shadowed entry and all its subordinates shall be shadowed."

This corrects the defects reported in defect report 9594/159.

Clause 19.3.2.2.1 Search procedure (I) , 1) b) i)

Replace the whole text of the clause 19.3.2.2.1 1) b) i) with the following text:

ii) If **e** is unsuitable, make a **continuationReference** as follows and add it to **SRContinuationList**:
- **targetObject** set to the DN of DSE e
- **operationProgress** with **nameResolutionPhase** set to **proceeding** and **nextRDNtoBeResolved** set to the number of RDNs in e

- all other components of **continuationReference** are unchanged

Then return.

In the note following clause 19.3.2.2.1.1) b) i), remove the brackets with their content.

Clause 18.3.1 Find DSE procedure

Delete in step 9) the first paragraph and the Note 3

This corrects the defects reported in defect report 9594/162.

Clause 20.4.5 APInfo procedure, 5) b) second last dash

*Replace "***chainingArguments.exclusions** absent*" by the following text:*

"**chainingArguments.exclusions** is set to either the relevant exclusions for the current target object if called by the Search Continuation Reference procedure, or absent if the APInfo procedure was called by the Name Resolution or the List Continuation procedures."

This corrects the defects reported in defect report 9594/180.

Clause 10.3 Chaining Arguments

Drop bullet g) which is a duplicate of o) and renumber the following clauses. Modify the order of m) n) and) o to o), n) m) which will become with the renumbering :

l) The **entryOnly** ...
m) **uniqueIdentifier**...
n) **authenticationLevel**...

This corrects the defects reported in defect report 9594/190.

Clause 19.3.1.2.2 List procedure (II), step 1b

In bullet 1) add a new step before a) and renumber the following steps:

c) If e′ is not an entry or alias, continue with the next immediate subordinate.
d) Check ACI ...

This corrects the defects reported in defect report 9594/198.

Clause 17.3.3.1 DUA request

Insert two new clauses e) and f) into 17.3.3.1 after bullet d) and renumber the existing e), f), g) to g),h),I) to read:

d) **ChainingArguments.AuthenticationLevel** and **ChainginArgument.UniqueID** are set according to the local security policy.

e) **ChainingArguments.nameResolveOnMaster** is copied from **CommonArguments.nameResolveOnMaster**.

f) **ChainingArguments.exclusions, ChainingArguments.entryOnly** and **ChainingArguments.referenceType** are copied from **CommonArguments.exclusions, CommonArguments.entryOnly** and **CommonArguments.referenceType** if they are present, otherwise they are omitted.

g) If the **manageDSAIT** option is set …

.

This corrects the defects reported in defect report 9594/206.

Clause 21 Results Merging procedure

Add the following note after bullet 6) :

> “Note : In case a DSA receives search or list results from other DSAs and such results have parameters unknown to the DSA, the uncorrelated results shall be returned. Otherwise, the DSA shall perform merging, if the search results are not signed.
>
> A DSA which received unsigned, uncorrelated results from a DSA not able to perform consolidation, shall perform merging, if it has the proper knowledge of all parameters of the uncorrelated results.”

This corrects the defects reported in defect report 9594/209.

Clause 12.1 Chained operations and Annex A

Modify as follows the ASN.1 of ERRORS :

ERRORS {operation.&Errors Except referrall dsaReferral}

Defect reports resolved by Draft Technical Corrigendum 2

(defect reports 211)

This corrects the defects reported in defect report 9594/211.

Clause 10.3

Change **timeLimit** *in* **ChainingArguments** *to:*

```
        timeLimit   [9]         Time OPTIONAL,
```

Insert the following after the ASN.1 definition of **ChainingArugments**

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

Add the following to k):

Before a value of **Time** is used in any comparison operation and if the syntax of **Time** has been chosen as the **UTCTime** type, the value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.

— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Note — The use of **GeneralizedTime** may prevent interworking with implementations unaware of the possibility of choosing either **UTCTime** or **GeneralizedTime**. It is the responsibility of those specifying the domains in which this Directory Specification will be used, e.g. profiling groups, as to when the **GeneralizedTime** may be used. In no case shall **UTCTime** be used for representing dates beyond 2049.

Also make theASN.1 changes to Annex A.

Recommendation X.518 (1997) | ISO/IEC 9594-4:1998 Technical Corrigendum 2

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 3, 4, and 5.

Defect reports resolved by Draft Technical Corrigendum 3

(defect reports 233 and 235)

This corrects the defects reported in defect report 9594/233.

In annex A:

Change all occurrences of **joint-iso-ccitt** to **joint-iso-itu-t**
add **enhancedSecurity** to the import from **UsefulDefinitions**
Add a semicolon to the end of import from **DirectoryAccessProtocol**.

This corrects the defects reported in defect report 9594/235.

Change 10.8 as follows:

10.8 Access point information

An **AccessPointInformation** value identifies one or more access points to the Directory.

AccessPointInformation ::= SET {
COMPONENTS OF MasterOrShadowAccessPoint,
additionalPoints [4] ~~SET OF~~ MasterAndOrShadowAccessPoints OPTIONAL }

In the case of 1988 edition DSAs producing an **AccessPointInformation** value, the optional component of the set is absent. In the case of 1988 edition DSAs interpreting an **AccessPointInformation** value, any **MasterAndShadowAccessPoints** value~~s~~ present is~~are~~ ignored.

In the case of post-1988 edition DSAs, the **MasterOrShadowAccessPoint** value component produced for an **AccessPointInformation** value may be of category master or shadow, as determined by the knowledge selection procedure of the DSA producing the value. It may be viewed as a suggested access point provided by the DSA generating the value to the DSA receiving it. A ~~set of~~ **MasterAndShadowAccessPoints** value~~s~~ may optionally also be produced for an **AccessPointInformation** value. This constitutes additional information which may be employed by the receiving DSA's knowledge selection procedure to determine an alternative access point.

Change the ASN.1 in Annex A

Defect reports resolved by Draft Technical Corrigendum 4

(defect report 234 and 248)

This corrects the defects reported in defect report 9594/234.
Delete the last sentence of 15.3.1 ("If protection is performed on the arguments, request decomposition shall not be used.")

This corrects the defects reported in defect report 9594/248.

In 25.1.4 and in Annex D replace:

```
NHOBSubordinateToSuperior  ::=  SubordinateToSuperior (
        WITH COMPONENTS { ..., alias ABSENT, entryInfo ABSENT})
```

with:

```
NHOBSubordinateToSuperior  ::= SEQUENCE {
        accessPoints    [0]         MasterAndShadowAccessPoints OPTIONAL,
        subentries                  [3]      SET OF SubentryInfo OPTIONAL }
```

Defect reports resolved by Draft Technical Corrigendum 5

(defect report 228, 242 and 265)

This corrects the defects reported in defect report 9594/228.

Delete the last paragraph of 16.3.9 and clause 21.

Delete any occurrence of

```
DIRQOP.&…-QOP{@dirqop},
```

Add to the start of 15.5.5:

Warning – This subclause refers to specifications that have been deprecated with respect to encryption. Signing of requests is not deprecated.

In Annex A, remove the **DIRQOP** *from the import*

This corrects the defects reported in defect report 9594/242.
Add size limit **SIZE (1..MAX)** to all optional **SET OF** and **SEQUENCE OF** constructs.

This corrects the defects reported in defect report 9594/265.
In 14.5, first paragraph, replace subordinate DSA *with* those DSAs.

Add a new paragraph and a note to the end of 15.3.1:
The **argument** of a chained request (see 12.1) or subrequest shall be the unmodified operation argument if the operation was initiated by a DUA. A DSA receiving a chained request shall not change **argument** when doing request decomposition.

NOTE – The following subclauses specifies that requirement for individual components of **argument**. This should not be interpreted to mean that component not explicitly mentioned can be changed.
In the start of the last paragraph of 15.5.2, add after "If a DSA encounters an extension": it does not support. *Change* execution phase *to* evaluation phase.

Delete 19.3.1.1.3.

Recommendation X.519 (1997) | ISO/IEC 9594-5:1998

Information processing systems - Open Systems Interconnection - The Directory - Protocol Specifications

TECHNICAL CORRIGENDUM 1

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 1.

Defect reports resolved by Draft Technical Corrigendum 1

This corrects the defect reported in defect report 9594/221.

Clause 9 Conformance

9.1 Conformance by DUAs

9.1.1 Statement Conformance

Add to 9.1.1 b)

and whether conformance for signed operations is claimed.

Add the following clause:

9.1.1 e) If conformance is claimed for strong authentication, signed operations, or protected operations, identification of the Certificate and CRL extensions for which conformance is claimed.

9.1.2 Static Conformance

Add the following clause:

9.1.2 d) conform to clause 12 of ISO/IEC 9594-8 | ITU-T Rec.X.509 for the Certificate and CRL extensions for which conformance was claimed in clause 9.1.1 e.

9.2 Conformance by DSAs

9.2.1 Statement Conformance

Add to 9.2.1 e):

and whether conformance for signed operations is claimed.

Add the following clause:

9.2.1 ad) If conformance is claimed for strong authentication, signed operations, or protected operations, identification of the Certificate and CRL extensions for which conformance is claimed.

9.2.2 Static Conformance

Add the following clause:

9.2.2 x) conform to clause 12 of ISO/IEC 9594-8 | ITU-T Rec.X.509 for the Certificate and CRL extensions for which conformance was claimed in 9.2.1 ad).

Recommendation X.519 (1997) | ISO/IEC 9594-5:1998 Technical Corrigendum 2

NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 2 and 3.

Defect reports resolved by Draft Technical Corrigendum 2

(defect report 236)

This corrects the defects reported in defect report 9594/236.

In Annex A, B, C, D imports:

Change **Remote-Operations-Realisations** and **realisations(8** or **9)** to **Remote-Operations-Realizations** and **realizations(9)**

Change

{joint-iso-ccitt remote-operations(4) remote-Operations-Abstract-Syntaxes(12) version1(0)}

to

{joint-iso-itu-t remote-operations(4) remote-operations-abstract-syntaxes(12) version1(0)}

In Annex A:

In the **DAP-Invokable OPERATION** construct replace **addEtry** with **addEntry**

In Annex C.

Replace **InvokeID** with **InvokeId**

In Annex D:

Change the object identifier for the module to:

{joint-iso-itu-t ds(5) module(1) dop(17) 3}

Annex G:

Changes to Annex G have been subsumed by the resolution to Defect Report 228.

Defect reports resolved by Draft Technical Corrigendum 3

(defect reports 228, 242 and 266)

This corrects the defects reported in defect report 9594/228.

In the **Introduction**, *delete the second last paragraph and change* Annex H *to* Annex G *in the last paragraph*.

In 2.1, delete references to Generic upper layers security

In clause 4, delete the GULS and SESE abbreviations.

Delete the last paragraph of 6.1.

In 6.7.3:

In the 3rd paragraph, delete "but not SESE".

In the 4th paragraph, replace "If the RTSE and SESE are both" *with* "If the RTSE is".

Delete the 5th and 6th paragraph including the two letter-numbered lists.

In 6.7.4:

In the 5th paragraph, delete "but not SESE".

In the 6th paragraph, replace "If the RTSE and SESE are both" *with* "If the RTSE is".

Delete the 7th and 8th paragraphs.

Delete 6.7.4

In 8.1.1, delete last paragraph.

In 8.1.1.1.2:

Delete in the first paragraph "if SESE is not used".
Delete last paragraph including its letter numbered list.

In 8.1.1.1.4, delete the last paragraph.

Delete 8.1.3.

In 8.2.1.1.2:

Delete "If SESE is not used,"
Delete the second (last) paragraph.

In 8.2.1.1.4:

Delete the single paragraph in this subclause.
Add a new paragraph instead:
The initiator of the association shall supply the Presentation Context Definition List in the **RT-OPEN** request primitive which shall contain the ACSE abstract-syntax (**id-as-acse**) and the DISP abstract-syntax that includes the RTSE (**id-as-directoryReliableShadowAS**).

Delete 8.2.3.

In 9.1.1:

In item a), delete "or **directoryAccessWith2or3seAC**"
Delete item e) and renumber next item.

In 9.1.2, item a), delete "or **directoryAccessWith2or3seAC**"

In 9.1.3, replace item a) with:

a) shall conform to the mapping onto the used service defined in clause 8 or clause 10 or both; and

In 9.2.1:

In item a), delete "**directoryAccessWith2or3seAC**, **directorySystemWith2or3seAC**,".
In item d), delete "or **directorySystemWith2or3seAC**".

In 9.2.3:

In item c), delete "or **directoryAccessWith2or3seAC**".
In item d), delete "or **directorySystemWith2or3seAC**".

In 9.3.1, item a), delete "**shadowSupplierInitiatedWith2or3seAC**, and **shadowConsumerInitiatedWith2or3seAC**".

In 9.4.1, item a), delete "**shadowSupplierInitiatedWith2or3seAC**, and **shadowConsumerInitiatedWith2or3seAC**".

In Annex A:

Remove **directorySecurityExchanges** *import from* **UsefulDefinitions**.
Delete the **id-ac-directoryAccessWith2or3seAC** *import from* **ProtocolObjectIdentifiers**
Delete the import from **directorySecurityExchanges**.
Delete the **directoryAccessWith2or3seAC** *application-context.*

In Annex B:

Remove **directorySecurityExchanges** *import from* **UsefulDefinitions**.
Delete the **id-ac-directorySystemWith2or3seAC** *import from* **ProtocolObjectIdentifiers**
Delete the import from **directorySecurityExchanges**.
Delete the **directorySystemWith2or3seAC** *application-context.*

In Annex C:

Remove **directorySecurityExchanges** *import from* **UsefulDefinitions**.
Delete the **id-ac-shadowSupplierInitiatedWith2or3seAC**, **id-ac-shadowConsumerInitiated-With2or3seAC**, **id-ac-reliableShadowSupplierInitiatedWith2or3seAC** *and* **id-ac-reliableShadowConsumerInitiatedWith2or3seAC** *imports from* **ProtocolObjectIdentifiers**
Delete the import from **directorySecurityExchanges**.

Delete the **shadowSupplierInitiatedWith2or3seAC**, **shadowConsumerInitiatedWith2or3seAC**, **reliableShadowSupplierInitiatedWith2or3seAC** *and* **reliableShadowConsumerInitiatedWith2or3seAC** *application-contexts.*

In Annex D:

Remove **directorySecurityExchanges** *import from* **UsefulDefinitions.**

Delete the **id-ac-directoryOperationalBindingManagementWith2or3seAC** *import from* **ProtocolObjectIdentifiers**

Delete the import from **directorySecurityExchanges.**

Delete the **directoryOperationalBindingManagementWith2or3seAC** *application-context.*

In Annex E:

Delete the **id-se** *import from* **UsefulDefinitions**

Delete the object identifiers **id-se-threewayse** and **id-se-spkmthreewayse.**

Delete Annex G and rename Annex H to Annex G.

This corrects the defects reported in defect report 9594/242.
Add size limit **SIZE (1..MAX)** to all optional **SET OF** and **SEQUENCE OF** constructs.

This corrects the defects reported in defect report 9594/266.
Reinstate the 9.1.1, item c) from edition 2 and changed the current item to d). Disregard the updates to 9.1.1 b) and 9.2.1 e) as required by Technical Corrigendum 1 to ITU-T Rec. X.519 (1997) | ISO/IEC 9594-5 : 1998.

Recommendation X.520 (1997) | ISO/IEC 9594-6:1998

Information processing systems - Open Systems Interconnection - The Directory - Selected Attribute Types

TECHNICAL CORRIGENDUM 1

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigendum 1.

Defect reports resolved by Draft Technical Corrigendum 1
(defect report 211)

This corrects the defects reported in defect report 9594/211.

Clause 6.3.2

Add the following to the last paragraph

The value of the two-digit year field shall be rationalized into a four-digit year value as follows:

— If the 2-digit value is 00 through 49 inclusive, the value shall have 2000 added to it.
— If the 2-digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

Recommendation X.520 (1997) | ISO/IEC 9594-6:1998 Technical Corrigendum 2

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 2 and 3.

Defect reports resolved by Draft Technical Corrigendum 2

(defect reports 237, 238 and 241)

This corrects the defects reported in defect report 9594/237.

In 5.2.1:

Replace the attribute definition with:

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

In 5.2.9:

The upper bound shall be **ub-serial-number** and the object identifier shall be **id-at-serialNumber**.

In 7.3:

Change **localeContextSyntax** to **LocaleContextSyntax** two places and remove the two spaces between "::" and **=**.
Add **{ub-locale-context-syntax}** after **DirectoryString**
The same changes have to be made to Annex A.
In Annex C add **ub-locale-context-syntax INTEGER ::= 64** to the end of the list.

In Annex A:

Remove **TeletexNonBasicParameters** from the import from **MTSAbstractService**
Remove one occurrence of **ub-name** from the import from **UpperBounds**
Add **CONTEXT** to the import from **InformationFramework**
In the **FacsimileTelephoneNumber** type definition, add a comma after **TelephoneNumber**.
In the **x121Address** attribute type definition, replace **X121.Address** with **X121Address**
In **X121Address** **::= NumericString (SIZE(1 ub-x121-address))** change the two spaces in the size specification to points, i.e. **SIZE(1..ub-x121-address)**
Add a right curly parenthesis at the end of the **languageContext** context definition.
Add a right curly parenthesis in the **Period** type as shown:

```
bitDay       BIT STRING { sunday (0), monday (1), tuesday (2),
             wednesday (3), thursday (4), friday (5), saturday (6) },
```

In the **NamedDay** type, replace **ENUMARATED** with **ENUMERATED**.
Add two hypens to the start of the second line of
-- id-at-encryptedTeletexTerminalIdentifier.
Add two hypens to the start of both lines of
-- *id-at-encryptedTeletexTerminalIdentifier*

In Annex C

:Change the last component of the object identifier for the module from **2** to **3**
The last occurrence **ub-name** shall be changed to **ub-surname**

This corrects the defects reported in defect report 9594/238.

In Clause 6.1.1 change in the first paragraph from:

attribute value of type **PrintableString**, **NumericString**, **TeletexString**, **BMPString**, **UniversalString**, or **DirectoryString**

to:

> attribute value of type **DirectoryString** and each data type appearing in the choice type **DirectoryString**, e.g. **UTF8String**.

In Clause 6.1.2 - 6.1.6 change in the first paragraph from:

> attribute value whose type is one of the ones listed in 6.1.1

to:

> attribute value of type **DirectoryString** and each data type appearing in the choice type **DirectoryString**, e.g. **UTF8String**.

This corrects the defects reported in defect report 9594/241.

In 5.2.9

> Replace "of a device" with "of an object"

Defect reports resolved by Draft Technical Corrigendum 3

(defect report 270)

This corrects the defects reported in defect report 9594/270.

In 5.8.1, replace ***caseIgnoreListMatch*** *matching rule with:*

```
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) }
```

In 6.1.10, replace ***caseIgnoreListMatch*** *matching rule with:*

```
        caseIgnoreListMatch  MATCHING-RULE  ::=  {
                SYNTAX        CaseIgnoreList
                ID            id-mr-caseIgnoreListMatch }

        CaseIgnoreList  ::=  SEQUENCE OF DirectoryString {ub-match}
```

Recommendation X.521 (1997) | ISO/IEC 9594-7:1998

Information processing systems - Open Systems Interconnection - The Directory – Selected object classes

TECHNICAL CORRIGENDUM 1

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigendum 1.

Defect reports resolved by Draft Technical Corrigendum 1

(defect report 239)

This corrects the defects reported in defect report 9594/239.

Add **certificateExtensions** to the import from **UsefulDefinitions**

Remove **supportedAlgorithms** and **deltaRevocationList** from the import from **AuthenticationFramework**

Add a new import:

```
supportedAlgorithms, deltaRevocationList
        FROM CertificateExtensions certificateExtensions   ;
```

Recommendation X.509 (1997) | ISO/IEC 9594-8:1998

Information processing systems - Open Systems Interconnection - The Directory - Authentication framework

TECHNICAL CORRIGENDUM 1

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 3, 4, 5, and 7.

Defect reports resolved by Draft Technical Corrigendum 3

(defect reports 200, 201, 212, 213, 218, and 220)

This corrects the defects reported in defect reports 9594/200.

Clause 12.6.2

Add the following at the end of the paragraph beginning with "If this extension is flagged critical":

"Where the distribution points are used to distribute CRL information for all revocation reason codes and all certificates issued by the CA include the **crlDistributionPoint** as a critical extension, the CA is not required to also publish a full CRL at the CA entry".

This corrects the defects reported in defect reports 9594/201.

Clause 12.6.3.1

Move the second sentence of the second paragraph *"If this field is absent …CRL issuer*" to the first paragraph immediately before the sentence "*This field is defined as follows*".

Add a paragraph break following the relocated sentence, making "*This field is defined as follows*" as an independent paragraph immediately before the ASN.1.

This corrects the defects reported in defect reports 9594/212.

Clause 12.7.6

Add the following to clause 12.7.6

g) **authorityKeyIdentifier** matches if the value of this component in the stored attribute value equals that in the presented value; there is no match if the stored attribute value contains no authority key identifier extension or if not all components in the presented value are present in the stored attribute value;

This corrects the defects reported in defect reports 9594/213.

Clause 12.7.6 d

Replace the text of 12.7.6 d with the following:

"d) **reasonFlags** matches if any of the bits that are set in the presented value are also set in the **onlySomeReasons** components of the issuing distribution point extension of the stored attribute value; there is also a match if the stored attribute value contains no **reasonFlags** in the issuing distribution point extension, or if the stored attribute value contains no issuing distribution point extension;

> Note: Even though a CRL matches on a particular value of **reasonFlags**, the CRL may not contain any revocation notices with that reason code."

This corrects the defects reported in defect reports 9594/218.

Clause 12.7.2 j)

Replace the text of 12.7.6 j with the following:

j) **policy** matches if at least one member of the **CertPolicySet** presented appears in the certificate policies extension in the stored attribute value; there is no match if there is no certificate policies extension in the stored attribute value;

This corrects the defects reported in defect reports 9594/220.

Clause 11.2 note 3

In Note 3, in the second sentence replace "*shall be absent*" with "*may be absent*".

In Note 3, at the beginning of the 3rd sentence, replace "*This may permit"* with *"If version is absent, this may permit"*

In Note 3, at the beginning of the 4th sentence, replace *"An implementation that supports version 2 (or greater) CRLs may"* with *"An implementation that supports version 2 (or greater) CRLs, in the absence of version, may also"*

Defect reports resolved by Draft Technical Corrigendum 4

(defect report 185)

This corrects the defects reported in defect reports 9594/185.

Clause 8

Add the following text immediately following the asn.1 for certificatePair

The **cACertificate** attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

The **forward** elements of the **crossCertificatePair** attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the **reverse** elements of the **crossCertificatePair** attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the **forward** and the **reverse** elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

When a **reverse** element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

In the case of v3 certificates, none of the above CA certificates shall include a **basicConstraints** extension with the **cA** value set to **FALSE**.

The definition of realm is purely a matter of local policy.

Also, replace Figure 4 with the following:

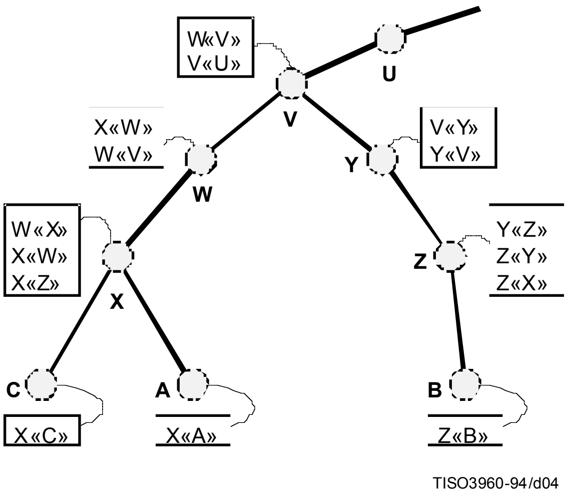


Figure 4: Certification path – hypothetical example

Defect reports resolved by Draft Technical Corrigendum 5

(defect reports 204)

This corrects the defects reported in defect reports 9594/204.

Clause 12.6.3.1

In the first sentence following the ASN.1, delete "unexpired"

Add the following as a new second sentence in the first paragraph following the ASN.1

"After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry."

Defect reports resolved by Draft Technical Corrigendum 7

(defect report 222)

This corrects the defects reported in defect report 222

Add the following to Section 12.1:

Certificate policy

The authentication framework contains three types of entity: the certificate user, the certification authority and the certificate subject (or end-entity). Each entity operates under obligations to the other two entities and, in return, enjoys limited warranties offered by them. These obligations and warranties are defined in a certificate policy. A certificate policy is a document (usually in plain-language). It can be referenced by a unique identifier, which may be included in the certificate policies extension of the certificate issued by the certification authority, to the end-entity and upon which the certificate user relies. A certificate may be issued in accordance with one or more than one policy. Definition of the policy, and assignment of the identifier, are performed by a policy authority. And the set of policies administered by a policy authority is called a policy domain. All certificates are issued in accordance with a policy, even if the policy is neither recorded anywhere nor referenced in the certificate. The standard does not prescribe the style or contents of the certificate policy.

The certificate user may be bound to its obligations under the certificate policy by the act of importing an authority public key and using it as a trust anchor, or by relying on a certificate that includes the associated policy identifier. The certification authority may be bound to ***its*** obligations under the policy by the act of issuing a certificate that includes the associated policy identifier. And, the end-entity may be bound to ***its*** obligations under the policy by the act of requesting and accepting a certificate that includes the associated policy identifier and by using the corresponding private key. Implementations that do not use the certificate policies extension should achieve the required binding by some other means.

For an entity to simply declare conformance to a policy does not generally satisfy the assurance requirements of the other entities in the framework. They require some reason to believe that the other parties operate a reliable implementation of the policy. However, if explicitly so stated in the policy, certificate users may accept the certification authority's assurances that its end-entities agree to be bound by their obligations under the policy, without having to confirm this directly with them. This aspect of certificate policy is outside the scope of the standard.

A certification authority may place limitations on the use of its certificates, in order to control the risk that it assumes as a result of issuing certificates. For instance, it may restrict the community of certificate users, the purposes for which they may use its certificates and/or the type and extent of damages that it is prepared to make good in the event of a failure on its part, or that of its end-entities. These matters should be defined in the certificate policy.

Additional information, to help affected entities understand the provisions of the policy, may be included in the certificate policies extension in the form of policy qualifiers.

Cross-certification

A certification authority may be the subject of a certificate issued by another certification authority. In this case, the certificate is called a cross-certificate, the certification authority that is the subject of the certificate is called the subject certification authority and the certification authority that issues the cross-certificate is called an intermediate certification authority (see Figure 1). Both the cross-certificate and the end-entity's certificate may contain a certificate policies extension.

The warranties and obligations shared by the subject certification authority, the intermediate certification authority and the certificate user are defined by the certificate policy identified in the cross-certificate, in accordance with which the subject certification authority may act as, or on behalf of, an end-entity. And the warranties and obligations shared by the certificate subject, the subject certification authority and the intermediate certification authority are defined by the certificate policy identified in the end-entity's certificate, in accordance with which the intermediate certification authority may act as, or on behalf of, a certificate user.

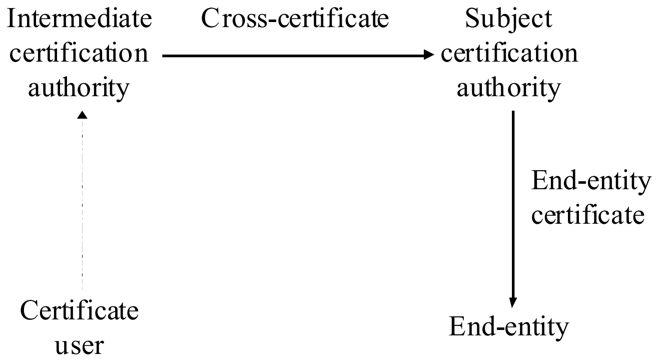

Intermediate certification authority
Cross-certificate
Subject certification authority
End-entity certificate
Certificate user
End-entity

Figure 1 - Cross-certification

A certification path is said to be valid under the set of policies that are common to all certificates in the path.

An intermediate certification authority may, in turn, be the subject of a certificate issued by another certification authority, thereby creating certification paths of length greater than two certificates. And, since trust suffers dilution as certificate paths grow in length, controls are required to ensure that end-entity certificates with an unacceptably low associated trust level will be rejected by the certificate user. This is part of the function of the certification path processing procedure.

In addition to the situation described above, there are two special cases to be considered:

1. the certification authority does not use the certificate policies extension to convey its policy requirements to certificate users; and

2. the certificate user or intermediate certification authority delegates the job of controlling policy to the next authority in the path.

In the first case, the certificate should not contain a certificate policies extension at all. As a result, the set of policies under which the path is valid will be null. But the path may be valid nonetheless. Certificate users must still ensure that they are using the certificate in conformance with the policies of the authorities in the path.

In the second case, the certificate user or intermediate certification authority should include the special value *any-policy* in the *initial-policy-set* or cross-certificate. Where a certificate includes the special value *any-policy*, it should not include any other certificate policy identifiers. The identifier *any-policy* should not have any associated policy qualifiers.

The certificate user can ensure that all its obligations are conveyed in accordance with the standard by setting the *initial-explicit-policy* indicator. In this way, only authorities that use the standard certificate policies extension as their way of achieving binding are accepted in the path, and certificate users have no additional obligations. Because authorities also attract obligations when they act as, or on behalf of, a certificate user, they can ensure that all their obligations are conveyed in accordance with the standard by setting **requireExplicitPolicy** in the cross-certificate.

Policy mapping

Some certification paths may cross boundaries between policy domains. The warranties and obligations according to which the cross-certificate is issued may be materially equivalent to some or all of the warranties and obligations according to which the subject certification authority issues certificates to end-entities, even though the policy authorities under which the two certification authorities operate may have selected different unique identifiers for these materially equivalent policies. In this case, the intermediate certification authority may include a policy mappings extension in the cross-certificate. In the policy mappings extension, the intermediate certification authority assures the certificate user that it will continue to enjoy the familiar warranties, and that it should continue to fulfill its familiar obligations, even though subsequent entities in the certification path operate in a different policy domain. The intermediate certification authority should include one or more mappings for each of a subset of the policies under which it issued the cross-certificate, and it should not include mappings for any other policies. If one or more of the certificate policies according to which the subject certification authority operates is identical to those according to which the intermediate certification authority operates (i.e. it has the same unique identifier), then these identifiers should be excluded from the policy mapping extension, but included in the certificate policies extension.

Policy mapping has the effect of converting all policy identifiers in certificates further down the certification path to the identifier of the equivalent policy, as recognized by the certificate user.

Policies should not be mapped either to or from the special value *any-policy*.

Certificate users may determine that certificates issued in a policy domain other than its own should not be relied upon, even though a trusted intermediate certification authority may determine its policy to be materially equivalent to its own. It can do this by setting the *initial-policy-mapping-inhibit input* to the path validation procedure. Additionally, an intermediate certification authority may make a similar determination on behalf of its certificate users. In order to ensure that certificate users correctly enforce this requirement, it can set inhibitPolicyMapping in a policy constraints extension.

Certification path processing

The certificate user faces a choice between two strategies:

1. it can require that the certification path be valid under at least one of a set of policies pre-determined by the user; or

2. it can ask the path validation module to report the set of policies for which the certification path is valid.

The first strategy may be most appropriate when the certificate user knows, a priori, the set of policies that are acceptable for its intended use.

The second strategy may be most appropriate when the certificate user does not know, a priori, the set of policies that are acceptable for its intended use.

In the first instance, the certification path validation procedure will indicate the path to be valid only if it is valid under one or more of the policies specified in the *initial-policy-set*, and it will return the sub-set of the *initial-policy-set* under which the path is valid. In the second instance, the certification path validation procedure may indicate that the path is invalid under the *initial-policy-set*, but valid under a disjoint set: the *authorities-constrained-policy-set*. Then the certificate user must determine whether its intended use of the certificate is consistent with one or more of the certificate policies under which the path ***is*** valid. By setting the *initial-policy-set* to *any-policy*, the certificate user can cause the procedure to return a valid result if the path is valid under any (unspecified) policy.

Self-issued certificates

There are three circumstances under which a certification authority may issue a certificate to itself:

1. as a convenient way of encoding its public key for communication to, and storage by, its certificate users;

2. for certifying key usages other than certificate and CRL signing (such as time-stamping); and

3. for replacing its own expired certificates.

These types of certificate are called self-issued certificates, and they can be recognized by the fact that the issuer and subject names present in them are identical. For purposes of path validation, self-issued certificates of type one are verified with the public key contained in them, and if they are encountered in the path, they shall be ignored.

Self-issued certificates of type two may only appear as end certificates in a path, and shall be processed as end certificates.

Self-issued certificates of type three (also known as self-issued intermediate certificates) may appear as intermediate certificates in a path. As a matter of good practice, when replacing a key that is on the point of expiration, a certification authority should request the issuance of any in-bound cross-certificates that it requires for its replacement public key before using the key. Nevertheless, if self-issued certificates are encountered in the path, they shall be processed as intermediate certificates, with the following exception: they do not contribute to the path length for purposes of processing the **pathLenConstraint** component of the **basicConstraints** extension and the *skip-certificates* values associated with the *policy-mapping-inhibit-pending* and *explicit-policy-pending* indicators."

In clause 12.2.2.6, after the 2nd sentence of the 1st paragraph, add the following:

The presence of this extension in an end-entity certificate indicates the certificate policies for which this certificate is valid. The presence of this extension in a certificate issued by one CA to another CA indicates the certificate policies for which this certificate can be used to validate certification paths.

Add the following text in clause 12.2.2.6, after the 1st sentence of the 1st paragraph.

The list of certificate policies is used in determining the validity of a certification path, as described in 12.4.3. The optional qualifiers are not used in the certification path processing procedure, but relevant qualifiers are provided as an output of that process to the certificate using application to assist in determining whether a valid path is appropriate for the particular transaction.

In clause 12.2.2.7, replace the sentence "This extension is always non-critical." with the following:

This extension may, at the option of the certificate issuer, be either critical or non-critical. It is recommended that it be critical, otherwise a certificate user may not correctly interpret the stipulation of the issuing CA.

Add the following new clause 12.4.2.4:

This field specifies a constraint that indicates any-policy is not considered an explicit match for other certificate policies for the remainder of the certification path.

```
inhibitAnyPolicy ::= EXTENSION {
        SYNTAX SkipCerts
IDENTIFIED BY {id-ce-inhibitAnyPolicy }}
```

This extension may, at the option of the certificate issuer, be either critical or non-critical. It is recommended that it be critical, otherwise a certificate user may not correctly interpret the stipulation of the issuing CA.

Add the following to the list of OIDs in the certificateExtensions module in Annex A:

```
id-ce-inhibitAnyPolicy          OBJECT IDENTIFIER ::= {id-ce 54}
```

Replace section 12.4.3 with the following:

12.4.3 Certification path processing procedure

Certification path processing is carried out in a system which needs to use the public key of a remote end entity, e.g. a system which is verifying a digital signature generated by a remote entity. The certificate policies, basic constraints, name constraints, and policy constraints extensions have been designed to facilitate automated, self-contained implementation of certification path processing logic.

The following is an outline of a procedure for validating certification paths. A conformant implementation shall be functionally equivalent to the external behaviour resulting from this procedure. But, the algorithm used by a particular implementation to derive the correct output(s) from the given inputs is not standardized.

The inputs to the certification path processing procedure are:

a) a set of certificates comprising a certification path;

b) a trusted public key value or key identifier (if the key is stored internally to the certification path processing module), for use in verifying the first certificate in the certification path;

c) an *initial-policy-set* comprising one or more certificate policy identifiers, indicating that any one of these policies would be acceptable to the certificate user for the purposes of certification path processing; this input can also take the special value *any-policy*;

d) an *initial-explicit-policy* indicator value, which indicates whether an acceptable policy identifier must appear in the certificate policies extension field of all certificates in the path;

e) an *initial-policy-mapping-inhibit* indicator value, which indicates whether policy mapping is forbidden in the certification path; and

f) the current date/time (if not available internally to the certification path processing module).

The values of c), d), and e) will depend upon the policy requirements of the user-application combination that needs to use the certified end-entity public key.

Note that because these are individual inputs to the path validation process, a certificate user may limit the trust it places in any given trusted public key to a given set of certificate policies. This can be achieved by ensuring that a given public key is the input to process only when initial-policy-set input includes policies for which the certificate user trusts that public key. Since another input to the process is the certification path itself, this control could be exercised on a transaction by transaction basis.

The outputs of the procedure are:

a) an indication of success or failure of certification path validation;

b) if validation failed, a diagnostic code indicating the reason for failure;

c) The set of authorities-constrained policies and their associated qualifiers in accordance with which the certification path is valid, , or the special value *any-policy*;

d) The set of user-constrained policies, formed from the intersection of the *authorities-constrained-policy-set* and the *initial-policy-set*;

e) *explicit-policy-indicator*, indicating whether the certificate user or an authority in the path requires that an acceptable policy be identified in every certificate in the path; and

f) details of any policy mapping that occurred in processing the certification path.

> NOTE — If validation is successful, the certificate-using system may still choose not to use the certificate as a result of values of policy qualifiers or other information in the certificate.

The procedure makes use of the following set of state variables:

a) *authorities-constrained-policy-set:* A table of policy identifiers and qualifiers from the certificates of the certification path (rows represent policies, their qualifiers and mapping history, and columns represent certificates in the certification path);

b) *permitted-subtrees*: A set of subtree specifications defining subtrees within which all subject names in subsequent certificates in the certification path must fall, or may take the special value *unbounded*;

c) *excluded-subtrees*: A (possibly empty) set of subtree specifications (each comprising a subtree base name and maximum and minimum level indicators) defining subtrees within which no subject name in a subsequent certificate in the certification path may fall;

d) *explicit-policy-indicator*: Indicates whether an acceptable policy must be explicitly identified in every certificate in the path;

e) *path depth*: An integer equal to one more than the number of certificates in the certification path for which processing has been completed;

f) *policy-mapping-inhibit-indicator*: Indicates whether policy mapping is inhibited;

g) *pending-constraints*: Details of explicit-policy and/or inhibit-policy-mapping constraints which have been stipulated but have yet to take effect. There are two one-bit indicators called *explicit-policy-pending*, and *policy-mapping-inhibit-pending* together with, for each, an integer called *skip-certificates* which gives the number of certificates yet to skip before the constraint takes effect.

The procedure involves an initialization step, followed by a series of certificate-processing steps. The initialization step comprises:

a) Write *any-policy* in the zeroth and first columns of the zeroth row of the *authorities-constrained-policy-set* table;

b) Initialize the *permitted-subtrees* variable to *unbounded*;

c) Initialize the *excluded-subtrees* variable to an empty set;

d) Initialize the *explicit-policy-indicator* to the *initial-explicit-policy* value;

e) Initialize *path-depth* to one;

f) Initialize the *policy-mapping-inhibit-indicator* to the *initial-policy-mapping-inhibit* value;

g) Initialize the two *pending-constraints* indicators to unset.

Each certificate is then processed in turn, starting with the certificate signed using the input trusted public key. The last certificate is considered to be the end certificate; any other certificates are considered to be intermediate certificates.

The following checks are applied to a certificate:

a) Check that the signature verifies, that dates are valid, that the certificate subject and certificate issuer names chain correctly, and that the certificate has not been revoked.

b) For an intermediate certificate, if the basic constraints extension field is present in the certificate, check that the **cA** component is present and set to true. If the **pathLenConstraint** component is present, check that the current certification path does not violate that constraint (ignoring intermediate self-issued certificates).

c) If the certificate policies extension is not present, then set the *authorities-constrained-policy-set* to null by deleting all rows from the *authorities-constrained-policy-set* table.

d) If the certificate policies extension is present and the value in *authorities-constrained-policy-set*[0, *path-depth*] is not *any-policy* and the value in the extension is not *any-policy*, then set the *authorities-constrained-policy-set* to the intersection of the *authorities-constrained-policy-set* with the set of policies present in the certificate. To do this, first add the policy qualifiers from the extension to the *authorities-constrained-policy-set* table by, for each policy identifier value in the extension, locate all rows in the *authorities-constrained-policy-set* table whose [*path-depth*] column entry contains the same value as that in the extension and attach the policy qualifiers from the extension to the policy identifiers in the table, then delete all rows for which the [*path-depth*] column did not contain one of the values in the extension.

e) If the certificate policies extension is present and the value in *authorities-constrained-policy-set*[0, *path-depth*] is not *any-policy* but the value in the extension is *any-policy*, then attach the policy qualifier (if present) from the extension to each policy identifier value in the [*path-depth*] column of the *authorities-constrained-policy-set* table.

f) If the certificate policies extension is present and the value in authorities-constrained-policy-set[0, path-depth] is any-policy, then set the authorities-constrained-policy-set to the intersection of the authorities-constrained-policy-set with the set of policies present in the certificate. To do this, add new rows to the table by duplicating the zeroth row a number of times equal to the number of policy identifiers in the extension minus one, and write the policy identifiers and qualifiers from the extension in authorities-constrained-policy-set[0, path-depth] and the path-depth column of each new row (this step must be performed even if the value in the extension is any-policy).

g) If the certificate is not an intermediate self-issued certificate, check that the subject name is within the name-space given by the value of permitted-subtrees and is not within the name-space given by the value of excluded-subtrees.

For an intermediate certificate, the following constraint recording actions are then performed, in order to correctly set up the state variables for the processing of the next certificate:

a) If the **nameConstraints** extension with a **permittedSubtrees** component is present in the certificate, set the *permitted-subtrees* state variable to the intersection of its previous value and the value indicated in the certificate extension.

b) If the **nameConstraints** extension with an **excludedSubtrees** component is present in the certificate, set the *excluded-subtrees* state variable to the union of its previous value and the value indicated in the certificate extension.

c) If policy-mapping-inhibit-indicator is set:

— process any policy mappings extension by, for each mapping identified in the extension, locate all rows in the *authorities-constrained-policy-set* table whose [*path-depth*] column entry is equal to the issuer domain policy value in the extension and delete the row.

d) If *policy-mapping-inhibit-indicator* is not set:

— process any policy mappings extension by, for each mapping identified in the extension, locate all rows in the *authorities-constrained-policy-set* table whose [*path-depth*] column entry is equal to the issuer domain policy value in the extension, and write the subject domain policy value from the extension in the [*path-depth*+1] column entry of the same row. If the extension maps an issuer domain policy to more than one subject domain policy, then the affected row must be copied and the new entry added to each row. If the value in *authorities-constrained-policy-set*[0, *path-depth*] is *any-policy*, then write each issuer domain policy identifier from the policy mappings extension in the [*path-depth*] column, making duplicate rows as necessary and retaining qualifiers if they are present, and write the subject domain policy value from the extension in the [*path-depth*+1] column entry of the same row.

— if the *policy-mapping-inhibit-pending* indicator is set and the certificate is not self-issued, decrement the corresponding *skip-certificates* value and, if this value becomes zero, set the *policy-mapping-inhibit-indicator*.

— If the **inhibitPolicyMapping** constraint is present in the certificate, perform the following. For a **SkipCerts** value of 0, set the *policy-mapping-inhibit-indicator*. For any other **SkipCerts** value, set the *policy-mapping-inhibit-pending* indicator, and set the corresponding *skip-certificates* value to the lesser of the **SkipCerts** value and the previous *skip-certificates* value (if the *policy-mapping-inhibit-pending* indicator was already set).

e) For any row not modified in either step c) or d), above (and every row in the case that there is no mapping extension present in the certificate), write the policy identifier from [path-depth] column in the [path-depth+1] column of the row.

f) Increment path-depth.

For all certificates, the following actions are then performed:

a) If explicit-policy-indicator is not set:

— if the *explicit-policy-pending* indicator is set and the certificate is not a self-issued intermediate certificate, decrement the corresponding *skip-certificates* value and, if this value becomes zero, set *explicit-policy-indicator*.

- If the **requireExplicitPolicy** component is present, and the certification path includes a certificate issued by a nominated CA, it is necessary for all certificates in the path to contain, in the certificate policies extension, an acceptable policy identifier. An acceptable policy identifier is the identifier of the certificate policy required by the user of the certification path, the identifier of a policy which has been declared equivalent to it through policy mapping, or any-policy. The nominated CA is either the issuer CA of the certificate containing this extension (if the value of **requireExplicitPolicy** is 0) or a CA which is the subject of a subsequent certificate in the certification path (as indicated by a non-zero value).

For the end-certificate, the following actions are then performed:

a) If explicit-policy-indicator is set, check that the authorities-constrained-policy-set table is not empty.If any of the above checks were to fail, then the procedure shall terminate, returning a failure indication, an appropriate reason code, explicit-policy-indicator and null values in the user-constrained-policy-set and the authorities-constrained-policy-set table.

If none of the above checks were to fail on the end certificate, then the *user-constrained-policy-set* shall be calculated by making a copy of the *authorities-constrained-policy-set* table, locating the left-most column whose zeroth row does not contain *any-policy* and deleting all rows which do not contain one of the identifiers in the *initial-policy-set* in this column. If all the columns contain *any-policy* in the zeroth row, then the table shall not be modified. Then the procedure shall terminate, returning a success indication together with the *explicit-policy-indicator*, the *authorities-constrained-policy-set* table and the *user-constrained-policy-set*.

The authorities-constrained-policy-set is the left-most column in the authorities-constrained-policy-set whose zeroth row does not contain the identifier any-policy. If there is no column that qualifies, then the authorities-constrained-*policy-set* is *any-policy*.

Recommendation X.509 (1997) | ISO/IEC 9594-8:1998
Technical Corrigendum 2

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 8 and 9.

Defect reports resolved by Draft Technical Corrigendum 8

(defect reports 226, 227 and 240)

This corrects the defects reported in defect report 226

In clause 11.2, delete the 2nd paragraph:

"The production of a certificate … compromise unlikely.".

This corrects the defects reported in defect report 227

In clause 12.2.2.1, add the following 2 sentences to the end of the paragraph that begins with "Certification authorities shall assign…"

"The **keyIdentifier** form can be used to select CA certificates during path construction. The **authorityCertIssuer**, **authoritySerialNumber** pair can only be used to provide preference to one certificate over others during path construction."

This corrects the defects reported in defect report 240

The following corrections should be made to the 1997 edition authenticationFramework module in Annex A of X.509:

1 Add "**id-mr**" to the list of objects imported from **UsefulDefinitions** module in the **authenticationFramework** module

2 Add "**AttributeType**", "**Attribute**", and "**MATCHING-RULE**" to the set of objects imported into the **authenticationFramework** module from the **InformationFramework** module.

3 Add "**GeneralNames**" to the set of objects imported into the **authenticationFramework** module from the CertificateExtensions module.

4 Consider adding the following definition to the **authenticationFramework** module because this is imported into other modules in the X.500 Series of Recommendations, but had never been included in the 97 text of X.509:

```
HASH {ToBeHashed} ::=  SEQUENCE {
      algorithmIdentifier        AlgorithmIdentifier,
      hashValue                  BIT STRING ( CONSTRAINED BY {
      -- must be the result of applying a hashing procedure to the
      -- DER-encoded octets of a value of --ToBeHashed } ) }
```

5 Add the following OID assignments in the **authenticationFramework** module:

```
id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::=
    {id-at 59}
id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::=
    {id-mr 42}
```

6 Add “**Time**” to the set of objects imported into the **certificateExtensions** module from the **authenticationFramework** module.

7 In the **certificateExtensions** module, and in the main text of X.509 clause 12.7.2, replace

```
CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId
```

with

```
CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
```

Defect reports resolved by Draft Technical Corrigendum 8

(defect reports 244, 256, 257 and 258)

This corrects the defects reported in defect report 244

In clause 8::

In the paragraph that begins "The extensions field allows addition of new ...", add the following two sentences to the end of the paragraph:

" When a certificate-using implementation recognizes and is able to process an extension, then the certificate-using implementation shall process the extension regardless of the value of the criticality flag. Note that any extension that is flagged non-critical will cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using that do not recognize the extension and will ignore it."

In clause 8:

Add the following immediately after the paragraph that begins "If unknown elements appear within the extension …":

A CA has three options with respect to an extension:

i) it can exclude the extension from the certificate;

ii) it can include the extension and flag it non-critical;

iii) it can include the extension and flag it critical.

A validation engine has two possible actions to take with respect to an extension:

i) it can ignore the extension and accept the certificate (all other things being equal);

ii) it can process the extension and accept or reject the certificate depending on the content of the extension and the conditions under which processing is occuring (e.g. the current values of the path processing variables).

Some extensions can only be marked critical. In these cases a validation engine that understands the extension, processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension rejects the certificate.

Some extensions can only be marked non-critical. In these cases a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension accepts the certificate (unless factors other than this extension cause it to be rejected).

Some extensions can be marked critical or non-critical. In these cases a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension, regardless of the criticality flag. A validation engine that does not understand the extension accepts the certificate if the extension is marked non-critical (unless factors other than this extension cause it to be rejected) and rejects the certificate if the extension is marked critical.

When a CA considers including an extension in a certificate it does so with the expectation that its intent will be adhered to wherever possible. If it is necessary that the content of the extension be considered prior to any reliance on the certificate, a CA would flag the extension critical. This must be done with the realization that any validation engine that does not process the extension will reject the certificate (probably limiting the set of applications that can verify the certificate). The a CA may mark certain extensions non-critical to achieve backward compatibility with validation applications that cannot process the extensions. Where the need for backward compatibility and interoperability with validation applications incapable of processing the extensions is more vital than the ability of the CA to enforce the extensions, then these optionally critical extensions would be marked non-critical. It is most likely that CAs would set optionally critical extensions as non-critical during a transition period while the verifiers' certificate processing applications are upgraded to ones that can process the extensions.

In clause 12.1:

In the paragraph that begins "In a certificate or CRL, an extension is flagged ...", add the following immediately after the third sentence that ends with "...ignoring the extension":

" If an extension is flagged non-critical, a certificate-using system that does recognize the extension, shall process the extension."

In clause 12.2.2.3:

In the paragraph that begins "If the extension is flagged non-critical ...", replace the second sentence with the following:

"If this extension is present, and the certificate-using system recognizes and processes the **keyUsage** extension type, then the certificate using system shall ensure that the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one."

In clause 12.2.2.4:

In the paragraph that begins "If the extension is flagged non-critical ...", replace the second sentence with the following:

"If this extension is present, and the certificate-using system recognizes and processes the **extendedKeyUsage** extension type, then the certificate using system shall ensure that the certificate shall be used only for one of the purposes indicated."

In clause 12.4.2.1:

In the 4th paragraph following the ASN.1, replace: "If this extension is present and is flagged critical then:" with the following:

"If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then:"

In clause 12.4.2.2:

Replace the last sentence "If this extension is present and is flagged critical ..." with the following:

"If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then the certificate-using system shall check that the certification path being processed is consistent with the value in this extension."

This corrects the defects reported in defect report 256

In clause 8:

In the first paragraph of the description of the cross certificate pair attribute (that begins "The forward elements …"), add the following as a new 3rd sentence.

"If a CA issues a certificate to another CA, and the subject CA is not a subordinate to the issuer CA in a hierarchy, then the issuer CA must place that certificate in the **reverse** element of the **crossCertificatePair** attribute of its own directory entry."

This corrects the defects reported in defect report 257

In clause 8 in the asn.1 construct ***CertificatePair,***

replace "**forward**" with "**issuedToThisCA**" and
replace "**reverse**" with "**issuedByThisCA**" and make changes to the associated text as outlined below.

In the descriptive text, throughout X.509, update the text accordingly to reflect these new terms. This includes the following specific clauses:

- *general descriptive text in clause 8,*
- *asn.1 and descriptive text for the cross certificate pair attribute in clause 8 ,*
- *asn.1 and descriptive text for the associated matching rules in clause 12.7.3 and 12.7.4 (1997) , and*

- *the duplicate asn.1 constructs in Annex A.*

Also, add the following text to the end of the first paragraph of clause 11.2.3:

The term **forward** was used in previous editions for **issuedToThisCA**, and the term **reverse** was used in previous editions for **issuedByThisCA.**

This corrects the defects reported in defect report 258

In clause 8, add the following as a new paragraph at the end of the clause, immediately before the first subclause (8.1):

"Each certificate in a certification path shall be unique. No certificate may appear more than once in a value of **theCACertificates** component of **CertificationPath** or in a value of **certificate** in the **CrossCertificates** component of **ForwardCertificationPath.**"

In clause 12.4.3 add the following note immediately after bullet a) a set of certificates …

"**Note**: A each certificate in a certification path is unique. A path that contains the same certificate two or more times is not a valid certification path."

Recommendation X.525 (1997) | ISO/IEC 9594-9:1998

Information processing systems - Open Systems Interconnection - The Directory - Replication

TECHNICAL CORRIGENDUM 1
NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigendum 1.

(defect reports 182, 186)

This corrects the defects reported in defect report 9594/182.

Clause 7.2.2.3

Insert as a fourth new paragraph

> If **subordinates** is specified, then the supplier shall send subordinate entries and a subordinate reference, and the SDSEs will be of type **subr**, **entry**, and **cp**. The subordinate entries shall contain attributes according to the attribute selection. In addition, if the supplying DSE is of type **admPoint**, then the SDSE shall additionally be of type **admPoint** and the **administrativeRole** attribute shall be supplied. All appropriate subentries, with only the appropriate information, below the **admPoint** DSE shall also be supplied as SDSEs in the shadowed information.

Clause 9.2 and Annex A

Replace the ***UnitOfReplication*** *ASN,1 type as follows (thereby adding* ***subordinates****):*

```
UnitOfReplication            ::=    SEQUENCE {
      area                          AreaSpecification,
      attributes                    AttributeSelection,
      knowledge                     Knowledge OPTIONAL,
      subordinates                  BOOLEAN DEFAULT FALSE }
```

Insert the following after the description of ***knowledgetype***

subordinates is used to indicate that subordinate entries, rather than simply subordinate references, are to be copied to the consumer DSA. **subordinates** may only be **TRUE** if **knowledge** is requested and **extendedKnowledge** is **FALSE**.

This corrects the defects reported in defect report 9594/186.

Clause 7.2.2.2

Append the following to a) in the fifth paragraph

If the **entryACI** operational attribute is present and holds relevant ACI, e.g. naming, then the attribute (containing at least the relevant ACI) shall always be included in the SDSE.

Clause 9.2.4.1

Add a new list element d)

d) If the entry is refined out, the replacement glue SDSE shall contain the necessary access control information.

Delete "prescriptive" from Note 2.

Recommendation X.525 (1997) | ISO/IEC 9594-9:1998 Technical Corrigendum 2

NOTE – This Technical corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 2, 3, and 4.

Defect reports resolved by Draft Technical Corrigendum 3

(Covering resolutions to defect report 187, 208 and 243)

This corrects the defects reported in defect report 9594/187.

In 7.2.1.1, add **root** to the list of SDSE types

In 11.3.1.1, delete **root** from the list of SDSE types

This corrects the defects reported in defect report 9594/208.

Insert the following text into 7.2.2.3, at the end of both the second paragraph and the first sentence of the third paragraph (after "appropriate knowledge"):

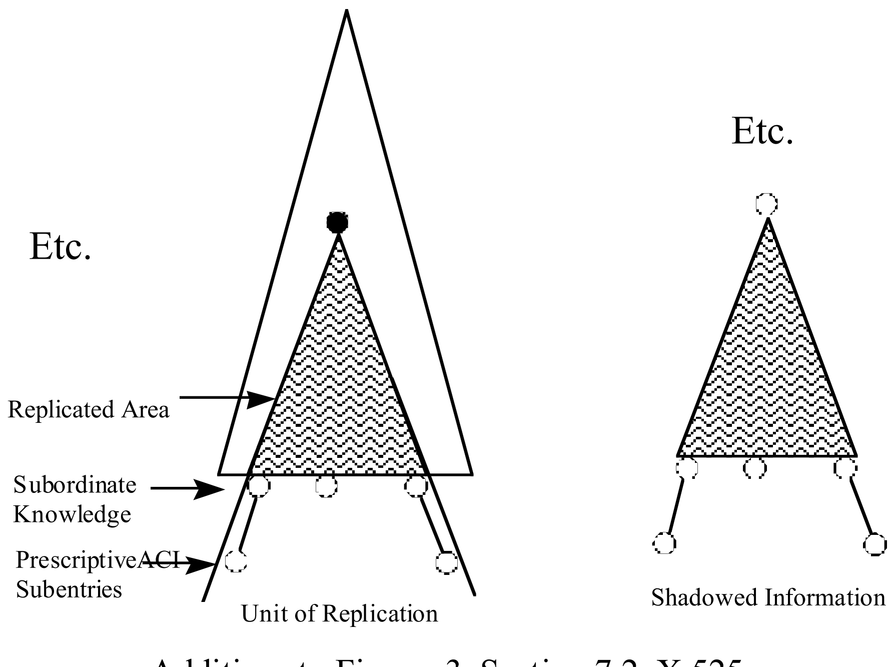
"and access control information."

Insert a new third paragraph into 7.2.2.3:

"If subordinate knowledge is supplied, and the supplying DSE (of type **subr)** is also of type **admPoint**, then the SDSE shall additionally be of type **admPoint** and the **administrativeRole** attribute shall be supplied. If such a DSE has any immediately subordinate subentries containing **PrescriptiveACI** relating to the administrative point, then they shall also be supplied as SDSEs in the shadowed information.

NOTE – A DSE can be of type **subr** and **admPoint** in a superior DSA, when the naming context in the subordinate DSA is the start of a new administrative area."

Update figure 3 to show a subentry immediately below a subordinate reference. The subentry contains prescriptiveACI and is part of the shadowed information.



Additions to Figure 3, Section 7.2, X.525

Add supporting text to section 7.2 in the paragraph after Figure 3. Insert after the sentence “Subordinate knowledge may also be replicated” the following sentences
“Implicit in the subordinate knowledge is the access control information which governs access to the RDN of the subordinate knowledge. When the subordinate entry is an administrative point in another DSA, then part of this access control information may be held in **prescriptiveACI** subentries beneath the subordinate knowledge.”

Add a new point d) to 9.2.4.1:
“if subordinate knowledge (not extended knowledge) is shadowed then any **prescriptiveACI** in subordinate subentries shall also be copied.”

This corrects the defects reported in defect report 9594/243.
In to 2.1, change all references ISO/IEC 9594-x:1997 *to* ISO/IEC 9594-x:1998
In clause 6, change ITU-T Rec. X.518| ISO/IEC 9594-5 *to* ITU-T Rec. X.519 | ISO/IEC 9594-5
In 9.2 in the **UnitOfReplication** *type, change* **ContextType** *to* **CONTEXT.&id.**
In 11.1:

> *change* **CoordinateShadowUpdate** *to* **coordinateShadowUpdate**
>
> *remove the last right curly parenthesis in the* **CoordinateShadowUpdateArgument**

Replace the ASN.1 in Annex A with:

```
DirectoryShadowAbstractService
        {joint-iso-itu-t ds(5) module(1) directoryShadowAbstractService(15) 4}
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

        directoryAbstractService, directoryOperationalBindingTypes, informationFramework,
        disp, distributedOperations, dsaOperationalAttributeTypes, enhancedSecurity,
        opBindingManagement

                FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 4}

        Attribute, AttributeType, CONTEXT, DistinguishedName, RelativeDistinguishedName,
        SubtreeSpecification
                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, directoryUnbind, 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

      id-errcode-shadowError, id-opcode-coordinateShadowUpdate, id-opcode-requestShadowUpdate,
      id-opcode-updateShadow, reliableShadowSupplierInitiatedAC, reliableShadowConsumerInitiatedAC,
      shadowConsumerInitiatedAC, shadowSupplierInitiatedAC
            FROM DirectoryInformationShadowProtocol disp
-- from ITU-T Rec. X.880 | ISO/IEC 13712-1

      ERROR, OPERATION
              FROM Remote-Operations-Information-Objects
                   {joint-iso-itu-t remote-operations(4) informationObjects(5) version1(0) }   ;

-- bind and unbind operations --

dSAShadowBind   OPERATION   ::=     directoryBind

dSAShadowUnbind        OPERATION   ::=        directoryUnbind

-- shadow operational binding --

shadowOperationalBinding OPERATIONAL-BINDING  ::=  {
      AGREEMENT                          ShadowingAgreementInfo
      APPLICATION CONTEXTS {
            { shadowSupplierInitiatedAC
              APPLIES TO          { All-operations-supplier-initiated } } |
            { shadowConsumerInitiatedAC
              APPLIES TO { All-operations-consumer-initiated } } |
            { reliableShadowSupplierInitiatedAC
              APPLIES TO { All-operations-supplier-initiated } } |
            { reliableShadowConsumerInitiatedAC
              APPLIES TO { All-operations-consumer-initiated } } }
      ASYMMETRIC
            ROLE-A  {      -- shadow supplier role
              ESTABLISHMENT-INITIATOR        TRUE
              ESTABLISHMENT-PARAMETER     NULL
              MODIFICATION-INITIATOR                          TRUE
              TERMINATION-INITIATOR             TRUE }
            ROLE-B        {           -- shadow consumer role
              ESTABLISHMENT-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,  -- must 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 34.2 b) and c) of CCITT Rec. X.208 and ISO/IEC 8824

-- 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 {
                greementID           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,
        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,
                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
```

Defect reports covered by Draft Technical Corrigendum 3

(defect report 245)

This corrects the defects reported in defect report 9594/245.

In 9.2, **UnitOfReplication**, change the **supplyContext** component to:

```
        supplyContexts              [0]     CHOICE {
                allContexts                 NULL,
                selectedContexts            SET OF CONTEXT.&id } OPTIONAL
```

Change **CommonResults** to **CommonResultSeq** in the import from **DirectoryAbstractService**.

In **CoordinateShadowUpdateResult**, **RequestShadowUpdateResult**, **UpdateShadowResult** and **shadowError** and associated text, change **CommonResults** to **CommonResultsSeq.**

(Changes to Annex A are subsumed by resolution to Defect Report 243)

Defect reports covered by Draft Technical Corrigendum 4

(defect reports 228 and 242)

This corrects the defects reported in defect report 9594/228.

Delete any occurrence of

```
                                    ,
        DIRQOP.&...-QOP{@dirqop}
```

In 11.1 change **CoordinateShadowUpdateResult** *to:*

```
CoordinateShadowUpdateResult  ::=  CHOICE {
        null            NULL,
        information             OPTIONALLY-PROTECTED { [0] SEQUENCE {
                greementID              AgreementID,
                lastUpdate                      Time OPTIONAL,
                COMPONENTS OF           CommonResultsSeq } } }
```

In 11.2 change **RequestShadowUpdateResult** *to:*

```
RequestShadowUpdateResult   ::=   CHOICE {
        null            NULL,
        information             OPTIONALLY-PROTECTED { [0] SEQUENCE {
                agreementID             AgreementID,
                lastUpdate                      Time OPTIONAL,
                COMPONENTS OF           CommonResultsSeq } } }
```

In 11.3 change **UpdateShadowResult** *to:*

```
UpdateShadowResult  ::=  CHOICE {
        null            NULL,
        information             OPTIONALLY-PROTECTED { [0] SEQUENCE {
                agreementID             AgreementID,
                lastUpdate                      Time OPTIONAL,
                COMPONENTS OF           CommonResultsSeq } } }
```

In clause 12 in the **shadowError** *construct, change* **OPTIONALLY-PROTECTED** *to* **OPTIONALLY-PROTECTED-SEQ.**

(Changes to Annex A are subsumed by resolution to Defect Report 243)

This corrects the defects reported in defect report 9594/242.

Add size limit **SIZE (1..MAX)** *to all optional* **SET OF** *and* **SEQUENCE OF** *constructs.*

Recommendation X.530 (1997) | ISO/IEC 9594-10:1998

Information processing systems - Open Systems Interconnection - The Directory – Use of systems management for administration of the Directory

TECHNICAL CORRIGENDUM 1
NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigendum 1.

Defect reports resolved by Draft Technical Corrigendum 1

(defect report 252)

This corrects the defects reported in defect report 9594/252.
In A.9:

Replace the module identification with:

```
DirectoryManagement {joint-iso-itu-t ds(5) module(1) directoryManagement(27) 1 }
```

Add **basicAccessControl** *and* **upperBounds** *to the import from* **UsefulDefinitions.**

Remove **ub-common-name** *from the import from* **SelectedAttributeTypes**

Add a new import:

```
ub-common-name
        FROM UpperBounds upperBounds
```

Remove **AttributeTypeAndValue** *from the import from* **InformationFramework**.

Replace:

```
Id-mat-foundLocalEntries                OBJECT IDENTIFIER       ::=     {id-mat 6}
```

with:

```
id-mat-foundLocalEntries                OBJECT IDENTIFIER       ::=     {id-mat 6}
```

Appendix C

Technical Corrigenda to Rec. X.500 (2000&2001) I ISO/IEC 9594 : 2000&2001 4th Edition

Summary of 4th Edition Technical Corrigenda

DTC #	Defect Reports resolved	Ballot Close	Published As	History
ITU-T Rec. X.501 (2001) I ISO/IEC 9594-2: 2001				
2-DTC1	250, 259	10 Jan 2001	4th edition	Erik after Orlando 2000. Incorporated into published edition.
ITU-T Rec. X.511 (2001) I ISO/IEC 9594-3: 2001				
3-DTC1	249, 262, 268	10 Jan 2001	4th edition	Erik after Orlando 2000. Incorporated into published edition.
ITU-T Rec. X.518 (2001) I ISO/IEC 9594-4: 2001				
4-DTC1	251, 253, 254, 264	10 Jan 2001	4th edition	Erik after Orlando 2000. Incorporated into published edition.
ITU-T Rec. X.519 (2001) I ISO/IEC 9594-5: 2001				
5-DTC1	271	10 Jan 2001	4th edition	Erik after Orlando 2000. Incorporated into published edition.

DTC #	Defect Reports resolved	Ballot Close	Published As	History
ITU-T Rec. X.520 (2001) I ISO/IEC 9594-6: 2001				
6-DTC2	251, 253, 270	10 Jan 2001	4th edition	Erik after Orlando 2000. Incorporated into published edition.
ITU-T Rec. X.509 (2000) I ISO/IEC 9594-8: 2000				
8-DTC1	244, 256, 257, 258	10 Jan 2001	4th edition	Sharon after Orlando 2000, comments resolved at Geneva 2001. Incorporated into published edition

All currently approved Technical Corrigenda to the 4th edition have been incorporated in the published edition.

Appendix D

Summary of Defect Reports

Defects numbered 001 to 074 apply to the 1988 edition only and are not documented here; for these see Version 9 of the Implementor's Guide. This is the last version that will document defect reports against the 1993 edition

All unmarked references to clauses and technical corrigenda are to the second (1993 / 1995) edition. This edition may also be explicitly identified as the second edition (2nd). The third edition (1997 / 1998) is identified by the mark 3rd. The 4th edition (2000 for X.509|9594-8 and 2001 for all others) is identified by the mark (4th).

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
075	Security levels	5/9.2.1.d	N1651	Japan	5-TC1
076	String attributes and spaces	6/6.2	N1664	UK	6-TC1
077	Bit ordering and DER	8/Annex D.4	N1874	UK	8-TC2
078	Use of term 'private key'	8/various	N1875	UK	8-TC2
079	*Hash functions*		*N1876*	*UK*	*Rejected*
080	Meaning of HASHED	8/Annex A.9	N1877	UK	**8-TC3(2nd)**
081	*Typing error*		*N1878*	*UK*	*Rejected*
082	*Padding conventions*		*N1879*	*UK*	*Rejected*
083	Transfer of key data	8/11.2.b	N1880	UK	8-TC2
084	Placement of certificates in the Directory	8/Scope	N1881	UK	8-TC2
085	Common arguments in List	3/10.1.2	N1882	UK	3-TC1

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
086	*Access control and aliases*		*N1883*	*UK*	*Rejected*
087	*Names for remove entry*		*N1884*	*UK*	*Rejected*
088	Absence of superior structure rule	2/12.6.5 and 2/12.6.6	N1885	UK	2-TC1
089	Creating administrative points	2/12.6.5 and 2/12.6.6	N1886	UK	2-TC1
090	New agreement parameter	2/24.3	N1887	UK	2-TC1
091	invalidID problem definition	2/24.5	N1888	UK	2-TC1
092	Encoding of signatures	8/Clause 9 & 8/Annex A	N1889	UK	**8-TC3 (2nd)**
093	*Typing error*		*N1890*	*UK*	*Rejected*
094	contextPrefixInfo	4/24.1.4.1.1	N1891	UK	4-TC1
095	*Typing error*		*N1892*	*UK*	*Rejected*
096	*Typing error*		*N1893*	*UK*	*Rejected*
097	Modification parameter for replication protocol	9/8.2.2.1 and 9/8.2.2.2	N1984	UK	9-TC1
098	*Inactive agreements*		*N1895*	*UK*	*Rejected*
099	Insufficient resources	9/Clause 12	N1896	UK	9-TC1
100	Canonical encodings	8/8.7	N1999	UK	**8-TC3(2nd)**
101	*Omission of userPassword*		*N2001*	*UK*	*Rejected*

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
102	Problems with structure rule	2/12.6.6	N2002	Australia	2-TC1
103	*ModifyDN with subordinates present*		*N2003*	*Australia*	*Rejected*
104	Aliased entry name	2/all	N2004	Australia	**3-TC2(2nd)**
105	*ModifyDN description errors*		*N2005*	*Australia*	*Rejected*
106	Already searched	410.4	N2006	Australia	4-TC1
107	*ASN.1 error*		*N2007*		*Rejected*
108	Common argument ignored	4/17.3.3.1	N2008	Australia	4-TC1
109	Find DSA procedure errors	4/18.3.1	N2009	Australia	4-TC1
110	*Target not found sub-procedure errors*		*N2010*	*Australia*	*Rejected*
111	Check suitability procedure errors	4/18.3.4.1	N2011	Australia	4-TC1
112	ModifyDN procedure errors	4/19.1.4	N2012	Australia	4-TC1
113	List procedure (I) errors	4/19.3.1.2.1	N2013	Australia	4-TC1
114	Search procedure (I) errors	4/19.3.2.2.1	N2014	Australia	4-TC1
115	Search procedure (II) errors	4/19.3.2.2.2	N2015	Australia	4-TC1
116	Checking trace information	4/19.3.2.2.3	N2016	Australia	**4-TC2(2nd)**
117	Repetitive chaining	4/Clause 20	N2017	Australia	**4-TC2(2nd)**
118	Avoiding duplicate results	4/20.1.1	N2018	Australia	**4-TC2(2nd)**

119	Looping involving referrals	4/15.4.2,
		4/16.1.2,
		4/20.4.5
			N2019	Australia	**3-TC2(2nd)**
					4-TC2(2nd)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
120	Duplicate removal in results merging	4/Clause 21	N2020	Australia	**4-TC2(2nd)**
121	General improvements to text	4/18.3.3(3), 4/19.3.2.2.1	N2021	Australia	**4-TC2(2nd)**
122	Matching rules for directory strings	6/6.1	N2022	Australia	6-TC1
123	Shadow operational binding	9/8.3	N2023	ITU Rapp.	9-TC1
124	ASN.1 tags for shadow operational binding	5/Annex D	N2024	ITU Rapp.	5-TC1
125	Matching rule description	2/14.7.3	N2025	ITU Rapp.	2-TC1
126	*Attribute syntax publication*		*N2026*	*ITU Rapp.*	*Rejected*
127	BMPString	6/Clause 5	N2027	ITU Rapp.	6-TC1 **3-TC2(2nd)**
128	Certificate extensibility	8/Clause 8	N2028	ISO Rapp.	8-TC1
129	*Changes to Modify Op Binding*			*UK*	*Rejected*
130	Clarification re Access Points	4/24.1.4.1.1, 4/24/1/4/2, 2/23		UK	**4-TC2(2nd)**
131	Incremental refreshes				*Rejected*
132	Consumer initiated updates	9/11/3/1		UK	**9-TC2(2nd)**
133	Critical extension bits	3/7.3.1		UK	**3-TC2(2nd)**
134	Version and Op Binding ID	2/24.2, 2/24.4			**2-TC2(2nd)**
135	UTC time matching	6/6.3.2		ITU Rapp.	**6-TC2(2nd)**
136	Min. no. of att values	2/8.2		UK	**2-TC2(2nd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
137	Access control flowcharts	3/Fig B-11		UK	**3-TC2(2nd)**
138	Access control flowcharts	3/Fig B-6		UK	**3-TC2(2nd)**
139	Application contexts for shadowing	5/7.2.3, 5/8.1.1.1.2, 5/9.3.1, 5/9.4.1		UK	**5-TC2(2nd)**
140	Hierarchical operational bindings	2/24		UK	**2-TC2(2nd)**
141	Prefix v policy information	9/9.2		UK	**9-TC2(2nd)**
142	Area specification	9/9.2		UK	**9-TC2(2nd)**
143	Absence of application component	2/14.7.4		Defect Group	**2-TC2(2nd)**
144	Extension of subschema modification procedure	2/14.5	8N362	Germany	**2-TC2(2nd)**
145	subtreeSpecification in subschema subentry	2/14.3	8N363	Germany	**2-TC2(2nd)**
146	Wrong upper bound for surname attribute	6/5.2.3, 6/AnnexA, 6/AnnexC	8N363	Germany	**6-TC2(2nd)**
147	Type reference and attribute syntax	2/14.7.4 note	8N363	Germany	**2-TC2(2nd)**
148	Inconsistencies in Search and List	3/10.1.2, 3/10.1.5, 3/10.2.3, 3/10.2.5	8N363	Germany	**3-TC2 (2nd)**
149	Matching rule distinguishedNameMatch	2/12.5.2	8N363	Germany	**2-TC2 (2nd)**
150	New update error: noSuchNewSuperior	3/11.4, 3/12.9	8N363	Germany	**3-TC2 (2nd)**
151	modifyDN on base of replicated area				*Rejected*

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
152	Wrong references	4/various	8N363	Germany	**4-TC2 (2nd)**
153	Error in figure: Operation dispatcher	4/Fig. 6	8N363	Germany	**4-TC2 (2nd)**
154	Arguments for Find DSE procedure	4/18.2.1, 4/18.3.4.1	8N363	Germany	**4-TC2 (2nd)**
155	Find DSE procedure	4/18.3.1	8N363	Germany	**4-TC2 (2nd)**
156	Figure in Add Entry procedure	4/19.1.1	8N363	Germany	**4-TC2 (2nd)**
157	ModifyDN and UnitOfReplication	4/19.1.4	8N363	Germany	**4-TC3 (2nd)** **4-TC1 (3rd)**
158	Errors in search procedure	4/19.3.2.1.3	8N363	Germany	**4-TC2 (2nd)**
159	targetObject in Search (I) procedure	4/19.3.2.2.1	8N363	Germany	**4-TC3 (2nd)** **4-TC1 (3rd**)
160	Collective attributes in Search (I) procedure	4/19.3.2.2.1	8N363	Germany	**4-TC2 (2nd)**
161	Search continuation reference procedure	4/20.4.4	8N363	Germany	**4-TC2 (2nd)**
162	APInfo procedure	4/20.4.5	8N363	Germany	**4-TC3 (2nd)** **4-TC1 (3rd)**
163	Shadowed information procedure	9/7.2, 9.Fig.3	8N363	Germany	**Accepted** Source solution
164	*ASN.1 of SupplierUpdateMode*				*Rejected*
165	Time limit in chaining arguments for modify or nssr	4/19.1.5	8N363	Germany	**4-TC2 (2nd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
166	Alias control by alias dereferencing	3/7.11.1	8N363	Germany	**3-TC3 (2nd)** **3-TC1 (3rd)**
167	Aliased RDNs in chaining args and cont. refs	4/10.3, 4/10.10, 4/18.3.1	8N363	Germany	**4-TC2 (2nd)**
168	*Protected password*				*Rejected*
169	Permutable property for PKCS	8/Clause 7, 8/10.2, 8/10.3		UK	**Accepted** **Not in DTC**
170	Entry selection in search procedure	3/Fig. B-11		UK	**Open**
171	Problems with Embedded PDV	2/12.4.6		ITU Rapp.	**2-TC2 (2nd)**
172	Subschema for the root entry and other problems	2/13.1		ITU Rapp.	**2-TC2 (2nd)**
173	NSSRs in the root entry	2/18.5		ITU Rapp.	**2-TC3 (2nd)** **2-TC1 (3rd)**
174	Service Errors and Operational Bindings	2/24.2-24.4		ITU Rapp.	**2-TC2 (2nd)**
175	Approximate match should imply equality	3/7.8.2f		ITU Rapp.	**3-TC2 (2nd)**
176	Access controls on aliases	3/7.11.1		ITU Rapp.	**Open**
177	Distinguished encoding of UTCTime	8/Clause 9		ISO Rapp.	**8-TC3**
178	Duplicate of 209				

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
179	Clarification in returnDN handling	2/Table K-1 3/7.4.11, B4, B5		Germany	**2-TC3 (2nd)** **2-TC1 (3rd)** **3-TC3 (2nd)** **3-TC1 (3rd)**
180	entryOnly inconsistency	3/7.3 4/10.3(g)-(o)		Germany	**Rejected** But editorial to part 4 was accepted - **4-TC3 (2nd)** **4-TC1 (3rd)**
181	*Shadowing access controls*				*Withdrawn*
182	Shadowing and one-level searching	9/7.2.2.3 and 9.2		IETF	**9-TC3 (2nd)** **9-TC1 (3rd)**
183	Public key usage	8/12.2.2..3		UK	**8-TC1 (3rd)**
184	*CertificationPath*	*8/8*		*UK*	***Rejected** Helsinki97*
185	Forward and reverse certificates	8/8		UK	**8-TC4 (3rd)**
186	Entry ACI and shadowing	9/7.2.2		UK	**9-TC3 (2nd)** **9-TC1 (3rd)**
187	sdseType of root	9/7.2.1.1		UK	**9-DTC2(3rd)**
188	Add permission and prescriptive ACI	3/11.1.5 (3)		UK	**3-TC3 (2nd)** **3-TC1 (3rd)**
189	Modify operational binding	2/24.3		UK	**2-TC3 (2nd)** **2-TC1 (3rd)**
190	Access controls	4/19.3.1.2.2 1b		UK	**4-TC3 (2nd)** **4-TC1 (3rd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
191	Alias loops	4/18.3.1		UK	**Rejected**
192	Collective attributes and content rules	2/11.7, 2/12.7.1, 2/13.6		UK	**Open**
193	*Policy constraints*				*Rejected*
194	Validity date	?			**8-TC1 (3rd)**
					8-TC3 (2nd)
195	Shadowing agreement parameters	9/9.1		UK	*Rejected*
196	*Validity period*				*Withdrawn*
197	DSE type bits	2/19.4.2		Defect Group	**Open**
		4/24.3.1.2			
198	Additions to chaining arguments	4/17.3.3.1		UK	**4-TC3 (2rd)** **4-TC1 (3rd)**
199	Presence Filter	3/7.8.2		US	**Accepted** with mod
					Not in DTC!!
200	CRL dist pts & full crls	8/12.6.2		Defect Group	**8-TC3 (3rd)**
201	Issuing distribution point	8/12.6.3.1		UK	**8-TC3 (3rd)**
202	Clarification of **CertificationPath** in **SecurityParameters**	3/7.10		Defect Group	**3-TC3 (2rd)** **3-TC1 (3rd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
203	Entry Information Selection	3/7.6		Defect Group	Rejected
204	Revoked certificates on CRL past expiry time	8/12.6.3.1 and 8/11.2		Defect Group	**8-TC5 (3rd)**
205	Definition of Superior Reference			US	**2-TC3 (2rd)** **2-TC1 (3rd)**
206	Handling extensions for search results	3/10.1.3 4/21		EIDQ/FDAS & ISSS/WS DIR	**3-TC3 (2rd)** **4-TC3 (2rd)** **3-TC1 (3rd)** **4-TC1 (3rd)**
207	Problem in the use of the Algorithm object Class	8/8 & Annex A		Rapporteur	**8-DTC6(97) ?**
208	Needed ACI when processing List using knowledge held in superior DSA	9/7.2.2.3 & 9.2.4.1		IETF IDS	**9-DTC2(3rd)**
209	DSA referrals (duplicate registration 178)			ITU rapporteur	**4-TC3 (2rd)** **4-TC1 (3rd)**
210	Shadowing attribute selection			Defect Group	**Open**
211	Y2K corrections	Parts 2, 3,4, & 6		US	**2-TC4, 3-TC4, 4-TC4, 6-TC3 for the 2nd edition 1993** **2-TC2, 3-TC3, 6-TC1 for the 3rd edition 1997**
212	CRL matching rules	8/12.7.6		US	**8-TC3 (3rd)**
213	CRL matching rules	8/12.7.6d		US	**8-TC3 (3rd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
214	Use of the term "canonical"	8/		Rapporteur	**8-DTC6(97) ?**
215	Access control to changing RDN			Rapporteur (UK)	**Open**
216	*CertificateAssertion*			*Australia*	***rejected***
217	Use of Operation and Error Code in Security Parameters	3/7.10		UK	**3-TC1 (3rd)**
218	Certificate Policy Match	8/12.7.2		UK	**8-TC3 (3rd)**
219	CA certificate and Basic Constraints	8/		IETF	***rejected***
220	CRL version number	8/		IETF/ISO rapporteur	**8-TC3 (3rd)**
221	Conformance for Certificate Extensions	5/9		Rapporteur's meeting	**5-TC1 (97 3rd)**
222	Policy Mapping	8/12.1 & 12.4.3		US (Santosh and Moses)	**8-TC7 (3rd)**
223	The naming attribute for an entry should always be shadowed.	9/9.2.2		UK	**Open**
224	The evaluation of a filter to UNDEFINED needs to be made consistent for the case where access control is/is not present.	3/7.8.2		UK	**3-DTC5(3rd)**
225	Entry Information Selection and **extraAttributes**	3/7.6		Australia	**Open**
226	CA system operational characteristics	8/11.2		Editor	**8-DTC8(3rd)**
227	Authority Key Identifier format	8/12.2.2.1		US	**8-DTC8(3rd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
228	ASN.1 errors in protection feature in X.501	2/15.3.2, P		Editor	**1-DTC1(3rd), 2-DTC4(3rd), 3-DTC5(3rd), 4-DTC5(3rd), 5-DTC3(3rd), 9-DTC4(3rd)**
229	Wrong references and minor ASN.1 errors in X.501	2/17.4.3, 18.1.2 – 3, B, F, P		Editor	**2-DTC3(3rd)**
230	**The X.501 ASN.1 type Issuer** is unknown	2/18.1.2.1		Editor	**2-DTC3(3rd)**
231	Simple credential ASN.1 error in X.511	3/8.1.1, A		Editor	**3-DTC3(3rd)**
232	Small ASN.1 editorial errors in X.511	3/7.2, 8.11, 9.3, A		Editor	**3-DTC3(3rd)**
233	Minor ASN.1 editorials in the import section of X.518 ASN.1 Module	4/ A		Editor	**4-DTC3(3rd)**
234	Wrong limitation on request decomposition	4/15.3.1		Editor	**4-DTC4(3rd)**
235	Error in X.518 ASN.1 datatype **AccessPointInformatio**n	4/10.8		Editor	**4-DTC3(3rd)**
236	Editorial mistakes in X.519 ASN.1 modules	5/A, B,C, D, G		Editor	**5-DTC2(3rd)**
237	ASN.1 errors in X.520	6/5.2.9, 7.6, A		Editor	**6-DTC2(3rd)**
238	Wrong reference of string types in X.520	6/6.1.1 - 6		Editor	**6-DTC2(3rd)**
239	Missing imports in X.521 ASN.1 module	7/A		Editor	**7-DTC1(3rd)**
240	Miscellaneous errors in X.509	A		Editor	**8-DTC8(3rd)**
241	SerialNumber attribute	6/5.2.9		Rapporteur	**6-DTC2(3rd)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
242	Size constraint on SET OF and SEQUENCE OF	8/		Rapporteur	**2-DTC4(3rd), 3-DTC5(3rd), 4-DTC5(3rd), 5-DTC3(3rd), 9-DTC4(3rd)**
243	Miscellaneous errors in X.525	9/2.1, 6, 9.2, 11.1-3, A		Editor	**9-DTC2(3rd)**
244	Clarification of conformance to criticality	8/see proposal		Sharon	**8-DTC9(3rd), 8-DTC1(4th)**
245	Duplicate Tags	9/9.2		Erik	**9-DTC3(3rd)**
246	Miscellaneous errors	6/5.12.2, 5.12.5, 6.8, A, C		Erik	
247	Miscellaneous errors	3/Introduction, 12.4		Erik	**3-DTC4(3rd)**
248	ASN.1 error in NHOBSubordinateToSuperior	4/25.1.4, D		Erik	**4-DTC4(3rd)**
249	Miscellaneous errors	3/3.7.4, 7.3.2, 7.7, 7.8.2, 7.8.3		Erik	**3-DTC1(4th)**
250	Miscellaneous errors	2/various		Erik	**2-DTC1(4th)**
251	**AdministrativeLimit**	4/16.1.4.4, 6/5.12.1		Erik	**4-DTC1(4th), 6-DTC1(4th)**
252	ASN.1 errors	10/A.9		Erik	**10-DTC1(3rd)**
253	Hierarchy selections problems	4/19.3.3.2.4 (old 19.3.3.2.1. 6/5.12.		Erik	**4-DTC1(4th), 6-DTC1(4th)**
254	**chainingRequired** component misplaced	4/10.4, 10.8, A		Erik	**4-DTC1(4th)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
255	Inconsistency in **CONTENT-RULE** information object class	2/12.7.2		Erik	**2-DTC4(3rd)**
256	Populating reverse element	8/		Sharon	**8-DTC9(3rd), 8-DTC1(4th)**
257	Renaming forward & reverse	8/		Sharon	**8-DTC9(3rd), 8-DTC1(4th)**
258	Certificate path loops	8/		Sharon	**8-DTC9(3rd), 8-DTC1(4th)**
259	**PartialOutcomeQualifier** and **ContextCombination** errors	4th 2/13.6.1, 16.10		Erik	**2-DTC1(4th)**
260	Ambiguity in **AttributeTypeAndDistinguishedValue**	2/9.3, B		Erik	**2-DTC4(3rd)**
261	**CommonResults** is wrong data dytpe	2/26.5		Erik	**2-DTC4(3rd)**
262	Signal hierarchy selection not supported	4th 3/13.3		Erik	**3-DTC1(4th)**
263	Incorrect clause references; test does not match ASN.1 for **SimpleCredentials**	3/7.1, 8.12		Erik	**3-DTC5(3rd)**
264	Optionally signal chaining; search constrained by service specific administrative area	4th 4/16.1.4.2, 19.3.2.2.4		Erik	**4-DTC1(4th)**
265	Various errors	4/14.5, 15.3.1, 19.3.1.1.3		Erik	**4-DTC5(3rd)**
266	Invalid updates of conformance clause	5/9		Erik	**5-DTC3(3rd)**
267	Various errors	2/14.7.3, 14.7.10, 25.2, 22.2.1.2		Erik	**2-DTC4(3rd)**
268	**noSubtypeSelection** in Entry information selection	4th 3/7.6		Erik	**3-DTC1(4th)**

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
269	Error in MatchingRuleDescription dasta type	2/12.5.2 b), 14.7.3		Erik	**2-DTC4(3rd)**
270	Data types in attribute syntaxes and matching rule assertion syntaxes	6/5.8.1, 6.1.1, 6.1.10, 6.5.3.1		Erik	**6-DTC3(3rd), 6-DTC1(4th)**
271	Use of term "packet"	4th 5/9.7		Erik	**5-DTC1(4th)**
272	Certification Path Length	3rd 8/12.4.2.1 & 4th 8/8.4.2, 15.5.2.1		Sharon	Solution being discussed
273	Name constraints conformance	3rd 12.4.2.2 4th 8.4.2.2		Sharon	Solution being discussed
274	Attribute Certificate version	4th 12.1, A		Sharon	Incorporated into published 4th edition
275	ExtendedKeyUsage	4th 8/8.4.2.1, 15.5.2.1		Sharon	Solution being discussed
276	Use of anyPolicy in self issued certificates	4th 8/8.1.5, 8.4.2.4, 10.5		Sharon	Solution being discussed
276	Requires explicit policy skip certificates value	4th 8/8.4.2.3, 10		Sharon	Solution being discussed

Appendix E

Defect Report Form

Please also send a soft copy of the defect in Microsoft Word format to the Defect Editor (hoytkesterson@earthlink.net).

DEFECT REPORT FORM

1. Defect Report Number:

   Title:

2. Source:

3. Addressed to: ISO/IEC JTC1/SC6 and ITU-T SG 7
   Editor Group on the Directory

4. (a) ISO/IEC JTC 1/SC 6 Secretariat: Fax: +82 2 369 8349
   Email: secretariat@jtc1sc06.org

   (b) ITU-T Study Group 7 Secretariat: Fax: +41 22 730 5853
   Email: sebek@itu.int

5. Date Circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:
   (number and title of IS or DIS final text/ITU Recommendation)

8. Qualifier: (e.g.: error, omission, clarification required)

9. References in Document: (e.g.: page, clause/section, figure, and/or table numbers)

10. Nature of Defect: (complete, concise explanation of the perceived problem)

11. Solution Proposed by the Source: (optional)

12. Editor's Response:

(any material proposed for processing as an erratum to, an amendment to, or a commentary on the IS or DIS final text/ITU Recommendation or Draft Recommendation is attached separately to this completed report).

Appendix F

Defect Resolution Committee Members

The following representatives have been nominated to the Collaborative Defect Resolution Committee.

International Defect Report Editor

Hoyt L. Kesterson II
7625 West Villa Rita Drive
Glendale, Arizona 85308
USA

Tel: +1 602 316 1985
Fax: +1 602 978 6750
Email: hoytkesterson@earthlink.net

Australia

Rolf Exner
Telstra Research Laboratories
770 Blackburn Road
Clayton Victoria 3168
Australia

Tel: +61 3 9253 6718
Fax: +61 3 9253 6352
Email: rolf.exner@team.telstra.com

Canada

Sharon Boeyen
Entrust Technologies
1000 Innovation Drive
Ottawa Ontario K2K 3E7
Canada

Tel: +1 613 270 3181
Fax: +1 613 270 2503
Email: boeyen@entrust.com

Denmark

Erik Andersen
Fischer & Lorenzo
Leopold Damms Alle 3
DK-2900 Hellerup
Denmark

Tel: +45 3947 0736
Fax: +45 3947 0777
Email: era.als@get2net.dk

France

Anh Hoang-Van
France Telecom
38-40, rue du General Leclerc
92131 Issy Les Moulineaux
France

Tel: +33 1 45 29 4597
Fax: +33 1 45 29 6531
Email: anh.hoang_van@issy.cnet.fr

Germany

Patrick Fantou
Siemens
ICN ISA TNA 4
Otto-Hahn-Ring 6
D-81739 Munich
Germany

Tel: +49 89 722 53243
Fax: +49 89 722 53249
Email: patrick.fantou@icn.siemens.de

Japan

(to be designated)

Norway

(to be designated)

Sweden
(to be designated)

United Kingdom
(to be designated)

United States of America

John (Skip) Slone
Lockheed Martin
MP 845
12506 Lake Underhill Road
Orlando, FL 32825
U.S.A.

Tel: +1 407 306 7102
Fax: +1 407 306 2023
Email: skip.slone@lmco.com