International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.518

Corrigendum 2

(10/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

Technical Corrigendum 2

Recommendation ITU-T X.518 (2008) – Technical Corrigendum 2

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	**X.500–X.599**
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems management framework and architecture	X.700–X.709
Management communication service and protocol	X.710–X.719
Structure of management information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, concurrency and recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599

For further details, please refer to the list of ITU-T Recommendations.

INTERNATIONAL STANDARD ISO/IEC 9594-4
RECOMMENDATION ITU-T X.518

Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

Technical Corrigendum 2

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.518	1988-11-25	
2.0	ITU-T X.518	1993-11-16	7
3.0	ITU-T X.518	1997-08-09	7
3.1	ITU-T X.518 (1997) Technical Cor. 1	2000-03-31	7
3.2	ITU-T X.518 (1997) Amd. 1	2000-03-31	7
3.3	ITU-T X.518 (1997) Technical Cor. 2	2001-02-02	7
4.0	ITU-T X.518	2001-02-02	7
4.1	ITU-T X.518 (2001) Technical Cor. 1	2005-05-14	17
4.2	ITU-T X.518 (2001) Cor. 2	2008-05-29	17
5.0	ITU-T X.518	2005-08-29	17
5.1	ITU-T X.518 (2005) Cor. 1	2008-05-29	17
5.2	ITU-T X.518 (2005) Cor. 2	2011-02-13	17
6.0	ITU-T X.518	2008-11-13	17
6.1	ITU-T X.518 (2008) Cor. 1	2011-02-13	17
6.2	ITU-T X.518 (2008) Cor. 2	2012-10-14	17
7.0	ITU-T X.518	2012-10-14	17

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

Technical Corrigendum 2

(covering resolution to defect reports 375, 376, 377, 380, 383, 384, 385, 386 and 387)

1) Correction of the defects reported in defect report 375

Change the second paragraph of item 1) in 16.1.4.2 as shown:

If the DSA using local knowledge knows, possibly reflected in the appropriate **MasterOrShadowAccessPoint** value, that chaining is required to the DSA to which an association is lost, it shall elect to send a **serviceError** with problem **unavailable**~~,~~. ~~and t~~The **notification** component of the **CommonResults** data type may be included and shall then contain:

– a **dSAProblem** notification attribute with the value **id-pr-targetDsaUnavailable**; and

– a **distinguishedName** attribute having as value the distinguished name of the DSA.

Change the second paragraph in 16.1.4.4 as shown:

Additional information may ~~shall~~ be returned by a DSA in a **dSAProblem** notification attribute as follows:

2) Correction of the defects reported in defect report 376

In 10.3 replace:

a) The **originator** component conveys the name of the (ultimate) originator of the request unless already specified in the security parameters. If **requestor** is present in **CommonArguments**, this argument may be omitted.

NOTE 1 – Where the originator has alternative names differentiated by context, then the name used as the value of **originator** shall be the primary distinguished name, if known. Otherwise, authentication and access control based on the value of **originator** may not work as desired.

with:

a) The **originator** component need not be present if the **requestor** component is present in **CommonArguments**, if the **certification-path** component is present in the **SecurityParameters** value, or if requestor information is only made available in the request, but not during the Bind operation. It shall not be present if requestor information is not available. It shall be present, if requestor information is only available as the result of the Bind operation.

3) Correction of the defects reported in defect report 377

In 10.3, replace:

n) **authenticationLevel** component is optionally supplied when it is required to indicate the manner in which authentication has been carried out. The **AuthenticationLevel** data type is described in ITU-T Rec. X.501 | ISO/IEC 9594-2.

with:

n) **authenticationLevel** component, when present, shall indicate the authentication level as established during the Bind operation. If this component is absent, a performing DSA shall assume that there has been no authentication (anonymous Bind). This component should be present whenever the requestor has been authenticated. The **AuthenticationLevel** data type is described in Rec. ITU-T X.501 | ISO/IEC 9594-2.

4) Correction of the defects reported in defect report 380

Update 10.3, item v) as shown:

v) The **dspPaging** component may be used to request DSP paging. If the bound DSA is different from the initial performer (see 15.5.5) and the bound DSA supports DSP paged results, it may set this component to **TRUE** to instruct the initial performer to provide DSP paged results. If this component is **FALSE** (default), the initial performer shall not perform DSP paged result. An initial performer that supports DSP paged results ~~performer~~ shall not forward this component to DSA(s) to which it is sending subrequests.

5) Correction of the defects reported in defect report 383

In 10.3, item h), delete the note and update as shown:

h) The **referenceType** component, when present, shall indicate~~s~~, to the DSA being asked to perform the operation, what type of knowledge was used to route the request to it. The DSA may therefore be able to detect errors in the knowledge held by the invoker. If such an error is detected, it shall be indicated by a **serviceError** with problem **invalidReference**. **ReferenceType** is specified fully in 10.7. If the **referenceType** is absent, the value **superior** shall be assumed.

In 10.3, item u), make the note to normal text:

In 10.11, update item b) as shown:

b) The **aliasedRDNs** component indicates how many (if any) of the RDNs in the target object name have been produced by dereferencing an alias. The argument is only present if an alias has been dereferenced.

NOTE – This component is provided for compatibility with first edition implementations of the Directory. ~~DUAs (and DSAs) implemented according to later editions of the Directory Specifications shall always omit this parameter from the CommonArguments of a subsequent request. In this way, the Directory will not signal an error if aliases dereference to further aliases.~~

This component shall not be included in **CommonArguments** when implementing according to the second or later editions of these Directory Specifications.

6) Correction of the defects reported in defect report 384

In 10.6, replace the text under the ASN.1 with:

Each DSA, which is propagating an operation to another DSA, shall add a new **TraceItem** to the end of the **TraceInformation**. Each such **TraceItem** value has the following components:

a) the **dsa** component that shall hold the name of the DSA which is adding the item;

b) the **targetObject** component, when present, shall be the value the DSA adding the item received on **targetObject** component of the **ChainingArguments** value of the incoming request. This parameter shall be omitted if:

- the request being chained came from a DUA, in which case its implied value is the **object** or **baseObject** in the DAP operation;
- the request is received from an LDAP client, in which case its implied value is the **object** or **baseObject** of the LDAP request; or
- if its value is the same as the (actual or implied) **targetObject** in the **ChainingArgument** of the outgoing request;

c) the **operationProgress** component shall have a value determined as follows:

- If the incoming request is received from a DUA, the value shall be taken from the **operationProgress** component of the **CommonArguments** of the DAP request. If this component is absent on the DAP request, the default value **notStarted** shall be used.
- If the incoming request is received from an LDAP client, the value **notStarted** shall be used.
- If the incoming request is received from a DSA, the value shall be taken from the **operationProgress** component of the **ChainedArguments** value. If this component is absent on the request, the default value **notStarted** shall be used.

7) Correction of the defects reported in defect report 385

In 3.7, add the following definition:

3.7.6 distributed directory: An interconnection set of a DSA and, in addition, one or more DSAs and/or LDAP servers.

In 15.1, change the first paragraph as shown:

Each DSA is equipped with procedures capable of completely fulfilling all Directory operations. In the case that a DSA contains the entire DIB, all operations are~~, in fact,~~ completely carried out within that DSA. In the case that the DIB is distributed across a distributed directory~~multiple DSAs~~, the completion of a typical operation is fragmented, with just a portion of that operation carried out in each of potentially many cooperating DSAs and LDAP servers.

8) Correction of the defects reported in defect report 386

Update 16.1.3 as shown:

16.1.3 Errors

At each stage of the processing, an error may be detected during the execution of any sub-procedure. The error identified within this sub-procedure is normally returned to the requestor as a corresponding protocol error. In this case, the **Operation Dispatcher** is terminated immediately. In the case that multiple errors are received, one shall be ~~local procedures may~~ selected ~~one of them~~ to be returned (see 12.1 of Rec. ITU-T X.511 | ISO/IEC 9594-3).

Alternatively, a procedure may choose to process errors (e.g., if a **serviceError** with problem **busy** is returned to a chained search subrequest) at certain points of operation processing. In this case, the procedure continues with its execution and no error is returned to the requestor.

The conditions under which a DSA may ~~optionally~~ sign the errors returned are specified in clause 12 of Rec. ITU-T X.511 | ISO/IEC 9594-3 ~~in a distributed operation based on error protection requested~~.

9) Correction of the defects reported in defect report 387

In 10.8 and Annex A, update as shown:

```
MasterOrShadowAccessPoint ::= SET {
  COMPONENTS OF AccessPoint,
  category            [3]  ENUMERATED {
    master               (0),
    shadow               (1),
    writeableCopy        (2) } DEFAULT master,
  chainingRequired    [5]  BOOLEAN DEFAULT FALSE }
```

In 10.8, item b), update as shown:

b) A **MasterOrShadowAccessPoint** value identifies an access point to the Directory. The **category**, either **master** or **shadow**, of the access point is dependent upon whether it points to a naming context or commonly usable replicated area. The **category writeableCopy** is only applicable if the access point is for an LDAP server with writeable copy entries. The **chainingRequired** component indicates whether chaining is required for that DSA, i.e., a referral shall not be returned for that DSA.

In 18.3.4, replace Figure 12 with Figure 12 from Rec. ITU-T X.518 (2001) | ISO/IEC 9594-4:2001.

In 18.3.4.1, update item 1) as shown:

1) If the DSE is not of type **shadow** ~~and it is not of type **writeableCopy**~~, then check if all **criticalExtensions** are supported. If they are, then return **entry suitable**, else return **unsupported critical extension**.

In 18.3.4.1, delete item 3) and shift numbering accordingly.

In 20.1.1, modify as shown:

20.1.1 Master only strategy

A DSA may choose this strategy to prevent the usage of shadowed information when performing a parallel or sequential multi-chaining caused by NSSR decomposition, or request decomposition during a Search or List evaluation. For this strategy, during a Search or List operation evaluation, the **excludeShadows** component of the **ChainingArguments** is set to **TRUE**. If NSSRs are encountered during Name Resolution, a DSA may set **nameResolveOnMaster** to **TRUE** to ensure that only a single path is followed. **nameResolveOnMaster** shall be set to **TRUE** if NSSRs are encountered and the operation is one of the Directory modification operations. In either case, only the DSA(s) that hold the ~~(primary)~~ master entry (or entries) relevant to the operation shall perform the operation. This master only strategy can be used during both parallel as well as sequential multi-chaining.

NOTE – Setting **nameResolveOnMaster** to **TRUE** eliminates the possibility of multiple paths during name resolution by:

1) ignoring shadow entries ~~and writeable copies of 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 ~~(primary)~~ 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.

Delete second paragraph of 22.1.2.

Delete clauses C.2.1, C.3.4, C.4 and C.5.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013