# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.518
**Corrigendum 1**
(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

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

**Technical Corrigendum 1**

Recommendation ITU-T X.518 (2008) – Technical Corrigendum 1

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.1598 |

*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 1

**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) Amend. 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 |

# CONTENTS

*Page*

**INTERNATIONAL STANDARD**
**RECOMMENDATION ITU-T**

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

## Technical Corrigendum 1

*(covering resolution to defect reports 338 and 339)*

## 1) Correction of the defects reported in defect report 338

*Delete 3.5 and renumber subsequent subclauses.*

*In 10.3 and Annex A: change the* **nonDapPdu** *and the* **streamedResults** *components to:*

```
  --                       [22] Not to be used
  -- streamedResults       [23] INTEGER OPTIONAL Currently not used
```

*Delete item w) and renumber subsequent items.*

*Add after new item w):*

> NOTE 6 – This component is currently not used. It might be used in the next edition of this Directory Specification. Otherwise, it will be deprecated.

*Modify 10.8 a) as follows:*

a) An **AccessPoint** value identifies a particular point at which access to the Directory, specifically to a DSA or LDAP server, can occur. When referring to a DSA, the access point shall have a **Name**, that of the DSA concerned~~, and may~~. It shall have a **PresentationAddress**, to be used in ~~OSI or IDM~~ communications to that DSA or LDAP server (see clause 11 of Rec. ITU-T X.519 | ISO/IEC9594-5 for additional information about NSAP formats).~~, in which case labeledURI shall not be present.~~

~~When referring to an LDAP server, the access point may have a labeledURI component, to be used in LDAP communications to that LDAP server. When the labeledURI component is present, the ae-title component and the address component and the protocolInformation component (if present) shall be ignored. This way of providing LDAP access point information is deprecated. Instead the format specified in 11.4 of ITU-T Rec. X.519 | ISO/IEC 9594-5 should be used. Also, in this case the ae-title and protocolInformation components shall be ignored.~~

```
AccessPoint  ::=  SET {
    ae-title                [0]  Name,
    address                 [1]  PresentationAddress,
    protocolInformation     [2]  SET SIZE (1..MAX) OF ProtocolInformation OPTIONAL,
    --                      [6]  Not to be used
}
    labeledURI              [6]  LabeledURI OPTIONAL }
LabeledURI  ::=  UnboundedDirectoryString
```

*Change the first paragraph of 12.1 as shown:*

A DSA, having received an operation from a DUA or LDAP client, may elect to construct a chained form of that operation to propagate to another DSA. A DSA, having received a chained form of an operation, may also elect to chain it to another DSA. The DSA invoking a chained form of an operation may sign~~, encrypt, or sign and encrypt~~ the argument of the operation; the DSA performing the operation, if so requested, may sign~~, encrypt, or sign and encrypt~~ the result or error returned by the responder of the operation. ~~A DSA, having received an operation from an LDAP client or having received an LDAP operation from another DSA, may elect to propagate the original LDAP client-supplied operation to an LDAP server.~~

*Change the following as shown:*

 a) **chainedArgument** – This is a value of **ChainingArguments** that~~which~~ contains ~~that~~ the information supplementing the information provided in the argument of ~~, over and above~~ the original DAP request~~UA- or LDAP client-supplied argument~~. This additional information is needed in order for the receiving to handle the operation properly~~, which is needed in order for the performing DSA or LDAP server to carry out the operation~~. This information type is defined in 10.3.

 b) **argument** – This is a value **operation.&Argument** and consists of the original DUA-supplied argument, as specified in the appropriate clause of ITU-T Rec. X.511 | ISO/IEC 9594-3~~, or the original LDAP client-supplied argument, as specified in the appropriate clause of IETF RFC 4510~~.

 > ~~NOTE 3 – It may also be possible to encapsulate PDU types other than those originating from DAP or LDAP if deemed appropriate. Specification of the mechanisms to do so is left for further study.~~

*In 13.1, replace the last sentence with:*

If an error occurs during a chained operation, the responding DSA may sign~~, encrypt, or sign and encrypt~~ the error returned.

*In 15.3.1, replace the second paragraph with:*

The **argument** of a chained request (see 12.1) or subrequest shall be the unmodified operation argument of the original DAP operation. ~~if the operation was initiated by a DUA and shall be the unmodified LDAPMessage if the operation was initiated by an LDAP client.~~ A DSA receiving a chained request shall not change **argument** when doing request decomposition.

*In 16.1.2, delete the last bullet of the list near the end of the subclause.*

*In 16.1.4.1, 16.2, 16.3.1, 16.3.4, 16.3.5, 16.3.6, 16.3.9, 17.1 and 17.2.2, remove references to LDAP and LDAP client.*

*In 17.3.3.1, remove the reference to LDAP client, and also in the heading.*

*Delete the last paragraph of current 17.3.3.3.*

*In 17.3.7, remove the reference to LDAP client.*

*In 18.2.1, delete as shown and renumber:*

The procedure uses the following arguments:

 a) ~~**ChainingArguments.traceInformation;**~~

 b) **ChainingArguments.aliasDereferenced;**

 c) **ChainingArguments.aliasedRDNs;**

 d) **ChainingArguments.excludeShadows;**

 e) **ChainingArguments.nameResolveOnMaster;**

 f) **ChainingArguments.operationProgress (nameResolutionPhase, nextRDNToBeResolved);**

 g) **ChainingArguments.referenceType;**

 h) **ChainingArguments.targetObject;**

 i) **ChainingArguments.relatedEntry;**

 j) ~~**ChainingArguments.streamedResults;**~~

 k) the operation type;

 l) the operation argument.

*In 18.2.4, change as shown:*

The procedure uses the following global variables:

 – **NRcontinuationList** list to store the Continuation Reference(s) needed to continue name resolution in the **Name Resolution Continuation Reference** procedure.

 – ~~**StreamedResultsOK** to store the determination of whether this DSA may chain streamed results in response to this operation.~~

*In 18.3.3, change item 2) as shown:*

2)  If the entry is suitable (**entry suitable**), then do the following:

   –   set **nameResolutionPhase** to **completed**;

   –   ~~compare the value in `ChainingArguments.streamedResults` (if present) with the number of elements in `ChainingArguments.traceInformation`; if equal, set `StreamedResultsOK` to true; and~~

   –   return **entry suitable**.

*In 19.3.2.2.1, change item 1) as shown:*

1)  If the **search** request is protected, generate a DSP request for each element of the **joinArguments** component each including the original DAP request ~~or LDAPMessage~~. The **ChainingArguments** shall be as follows:

*In 22.1.1, change item 2) as shown:*

   –   The DSA with which the DUA ~~or LDAP client~~ association exists shall insert the requester's distinguished name in the initiator field of the **ChainingArguments** for all subsequent chained operations to other DSAs.

*In 22.2, first paragraph, remove the reference to LDAP client.*


## 2)       Correction of the defects reported in defect report 339

*Make the following changes to 11.1 of Rec. ITU-T X.518 | ISO/IEC 9594-4:*

### 11.1       DSA Bind

### 11.1.1       DSA Bind syntax

A ~~Dd~~SABind operation is used to begin a period of cooperation between two DSAs providing the Directory service.

```
DdSABind   ::=   BINDOPERATION   {
    ARGUMENT        DSAirectoryBindArgument
    RESULT          DSAirectoryBindResult
    BIND ERRORS     { DdirectoryBindError } }

DSABindArgument  ::=  SET  {
    credentials     [0]  DSACredentials OPTIONAL,
    versions        [1]  Versions DEFAULT {v1} }

DSACredentials  ::=  CHOICE {
    simple              [0]  SimpleCredentials,
    strong              [1]  StrongCredentials,
    externalProcedure   [2]  EXTERNAL,
    spkm                [3]  SpkmCredentials }

DSABindResult  ::=  DSABindArgument
```

### 11.1.2       DSA Bind arguments

The components of the **DSABindArgument** are identical to their counterparts in the **DirectoryBindArgument** (see ITU-T Rec. X.511 | ISO/IEC 9594-3) with the following differences:

   –   The **Credentials** of the **DirectoryBindArgument** allows information identifying the AE-Title of the initiating DSA to be sent to the responding DSA. The AE-Title shall be in the form of a Directory Distinguished Name.

       The **SaslCredentials** are not included in the **Credentials**.

   –   The **Credentials** of the **DirectoryBindResult** allows information identifying the AE-Title of the responding DSA to be sent to the initiating DSA. The AE-Title shall be in the form of a Distinguished Name.

   –   The DSA's name or AE-Title may use alternative distinguished names and may include context information.

NOTE 1— Where names are used in either simple or strong credentials, it is possible to use alternative distinguished names, if they exist. However, authentication and access control based on the name may not work as desired if the primary distinguished name is not used. Following successful processing of an authenticated BIND operation, whatever the name used in the BIND argument, the bound entities shall thereafter know each other by their primary distinguished names, to facilitate operation of access controls while the BIND is in effect.

### 11.1.3    Directory Bind results

The components of the `DSABindResult` are identical to their counterparts in the `DirectoryBindResult` (see Rec. ITU-T X.511 | ISO/IEC 9594-3) with the following differences:

–    The `Credentials` of the `DirectoryBindResult` allows information identifying the AE-Title of the responding DSA to be sent to the initiating DSA. The AE-Title shall be in the form of a Distinguished Name.

The `SaslCredentials` are not included in the `Credentials`.

### 11.1.4    DSA Bind errors

Should the Bind request fail, a bind error shall be returned. If the Bind request was either using strong authentication or SPKM credentials are supplied, then the Bind responder may sign the error parameters.

The `versions` parameter of the `dSABindError` indicates which versions are supported by the responding DSA.

The `SecurityParameters` components (see 7.10 of Rec. ITU-T X.511 | ISO/IEC 9594-3) shall be included if the error is to be signed.

A `securityError` or `serviceError` shall be supplied as follows:

–    `securityError`    `inappropriateAuthentication`
                        `invalidCredentials`
                        `blockedCredentials`

–    `serviceError`    `unavailable`

*Make the following changes to Annex A of Rec. ITU-T X.518 | ISO/IEC 9594-4:*

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

    abandon, addEntry, CommonResults, compare, directoryBindError, list,
    modifyDN, modifyEntry, read, referral, removeEntry, search, SecurityParameters,
    SimpleCredentials, SpkmCredentials, StrongCredentials, Versions
        FROM DirectoryAbstractService directoryAbstractService

-- bind unbind operation --

dSABind              OPERATION  ::=  directoryBind

dSABind  OPERATION  ::=  {
    ARGUMENT   DSABindArgument
    RESULT     DSABindResult
    ERRORS     { directoryBindError } }

DSABindArgument  ::=  SET  {
    credentials     [0]  DSACredentials OPTIONAL,
    versions        [1]  Versions DEFAULT {v1} }

DSACredentials  ::=  CHOICE  {
    simple            [0]  SimpleCredentials,
    strong            [1]  StrongCredentials,
    externalProcedure [2]  EXTERNAL,
    spkm              [3]  SpkmCredentials }

DSABindResult  ::=  DSABindArgument
```

# 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