Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14279
Date:	2010-04-28
Replaces:	
Document Type:	Text for DCOR ballot
Document Title:	Text for DCOR ballot, ISO/IEC 9594-4:2005 Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation, ITU-T X.518 (2005)
Document Source:	SC 6/WG 8 Geneva meeting
Project Number:	
Document Status:	SC 6 P-members are requested to ballot on this DCOR text through the e-balloting system (www.iso.org/jtc1/sc6) no later than 2010-07-28.
Action ID:	LB
Due Date:	2010-07-28
No. of Pages:	5

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

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

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

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

ITU-T X.518 (2005) | ISO/IEC 9594-4:2005
Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

Technical Corrigendum 2

(covering resolution to defect reports 338, 339 and 345)

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 streamResults components to:

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

Delete item w and renumber subsequent items.):

Add after new 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.

Change 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** which contains that information, over and above the original DUA- or LDAP client-supplied argument, 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 16.1.2 delete the last bullet of the list near the end of the subclause.

In 16.1.4, 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 13.3.3.1, remove reference to LDAP client, also in heading and delete bullets k) and l).

Delete 17.3.3.2 and renumber subsequent subclauses.

Delete the last paragraph of current 17.3.3.3.

In 17.3.7, remove 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 1 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 reference to LDAP client.

2) Correction of the defects reported in defect report 339

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

11.1.1 DSA Bind syntax

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

```
~~D~~dSABind  ::=  ~~BIND~~OPERATION  {
     ARGUMENT        DSA~~irectory~~BindArgument
     RESULT               DSA~~irectory~~BindResult
     ~~BIND~~ ERRORS           { ~~D~~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
```

11.1.2 DSA Bind arguments

The components of the **DSABind**`Argument` are identical to their counterparts in the **DirectoryBind**`Argument` (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.

~~NOTE 2 – The credentials required for authentication may be carried by the Security Exchange Service Element (see ITU-T Rec. X.519 | ISO/IEC 9594-5) in which case they are not present in the bind arguments or results.~~

11.1.3 Directory Bind results

The components of the `DSABindResult` are identical to their counterparts in the `DirectoryBindResult` (see ITU-T Rec. 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 ITU-T Rec. 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 ITU-T Rec. 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 }
```

3) Correction of the defects reported in defect report 345

In 11.2, change 9.3.2 of ITU-T Rec. X.519 | ISO/IEC 9594-5 *to* 9.2.2 of ITU-T Rec. X.519 | ISO/IEC 9594-5.

_____