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

TECHNICAL CORRIGENDUM 2

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Procédures pour le fonctionnement réparti

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to ISO/IEC 9594-4:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, Telecommunications and information exchange between systems, in collaboration with ITU-T. The identical text is published as Rec. ITU T X.518 (2005)/Cor.2 (02/2011).
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. It shall have a PresentationAddress, to be used in communications to that DSA or LDAP server (see clause 11 of ITU-T Rec. X.519 | ISO/IEC 9594-5 for additional information about NSAP formats).
```

Replace the AccessPoint data type with:

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

Change the first paragraph of 12.4 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 supplementing the information provided in the argument of the original DAP request. This additional information is needed in order for the receiving to handle the operation properly, 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 \texttt{operationArgument} 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.

\textbf{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.

\textit{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.

\textit{In 15.3.1, replace the second paragraph with:}

The \textit{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 \textit{argument} when doing request decomposition.

\textit{In 16.1.2, delete the last bullet of the list near the end of the subclause.}

\textit{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.}

\textit{In 17.3.3.1, remove the reference to LDAP client, and also in the heading.}

\textit{Delete the last paragraph of current 17.3.3.3.}

\textit{In 17.3.7, remove the reference to LDAP client.}

\textit{In 18.2.1, delete as shown and renumber:}

The procedure uses the following arguments:

\begin{itemize}
\item a) \texttt{ChainingArguments.traceInformation},
\item b) \texttt{ChainingArguments.aliasDereferenced},
\item c) \texttt{ChainingArguments.aliasedRDNs},
\item d) \texttt{ChainingArguments.excludeShadows},
\item e) \texttt{ChainingArguments.nameResolveOnMaster},
\item f) \texttt{ChainingArguments.operationProgress} (nameResolutionPhase, nextRDNToBeResolved);
\item g) \texttt{ChainingArguments.referenceType},
\item h) \texttt{ChainingArguments.targetObject},
\item i) \texttt{ChainingArguments.relatedEntry},
\item j) \texttt{ChainingArguments.streamedResults};
\item k) the operation type;
\item l) the operation argument.
\end{itemize}

\textit{In 18.2.4, change as shown:}

The procedure uses the following global variables:

\begin{itemize}
\item \texttt{NRcontinuationList} list to store the Continuation Reference(s) needed to continue name resolution in the Name Resolution Continuation Reference procedure.
\item \texttt{StreamedResultsOK} to store the determination of whether this DSA may chain streamed results in response to this operation.
\end{itemize}

\textit{In 18.3.3, change item 2) as shown:}

\begin{itemize}
\item 2) If the entry is suitable \textit{(entry suitable)}, then do the following:
\begin{itemize}
\item set \texttt{nameResolutionPhase} to \texttt{completed};
\item compare the value in \texttt{ChainingArguments.streamedResults} (if present) with the number of elements in \texttt{ChainingArguments.traceInformation}; if equal, set \texttt{StreamedResultsOK} to \texttt{true}; and
\item return \textit{entry suitable}.
\end{itemize}
\end{itemize}
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 \texttt{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 D\texttt{dSABind} operation is used to begin a period of cooperation between two DSAs providing the Directory service.

\begin{verbatim}
\texttt{DdSABind ::= BINDOPERATION { \\
\hspace{1em} ARGUMENT DSAirectoryBindArgument \\
\hspace{1em} RESULT DSAirectoryBindResult \\
\hspace{1em} BIND-ERRORS { DdirectoryBindError } } }
\end{verbatim}

\begin{verbatim}
\texttt{DSABindArgument ::= SET { \\
\hspace{1em} credentials [0] DSACredentials OPTIONAL, \\
\hspace{1em} versions [1] Versions DEFAULT {v1} } }
\end{verbatim}

\begin{verbatim}
\texttt{DSACredentials ::= CHOICE { \\
\hspace{1em} simple [0] SimpleCredentials, \\
\hspace{1em} strong [1] StrongCredentials, \\
\hspace{1em} externalProcedure [2] EXTERNAL, \\
\hspace{1em} spkm [3] SpkmCredentials } }
\end{verbatim}

\begin{verbatim}
\texttt{DSABindResult ::= DSABindArgument}
\end{verbatim}

11.1.2 DSA Bind arguments

The components of the DSA\texttt{BindArgument} are identical to their counterparts in the Directory\texttt{BindArgument} (see ITU-T Rec. X.511 | ISO/IEC 9594-3) with the following differences:

– The \texttt{Credentials} of the Directory\texttt{BindArgument} 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 \texttt{SaslCredentials} are not included in the \texttt{Credentials}.

– The \texttt{Credentials} of the Directory\texttt{BindResult} 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 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.511 | 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,

FROM DirectoryAbstractService directoryAbstractService

-- bind unbind operation --

dSABind OPERATION ::= directoryBind

dSABind OPERATION ::= directoryBind

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

3) Correction of the defects reported in defect report 345