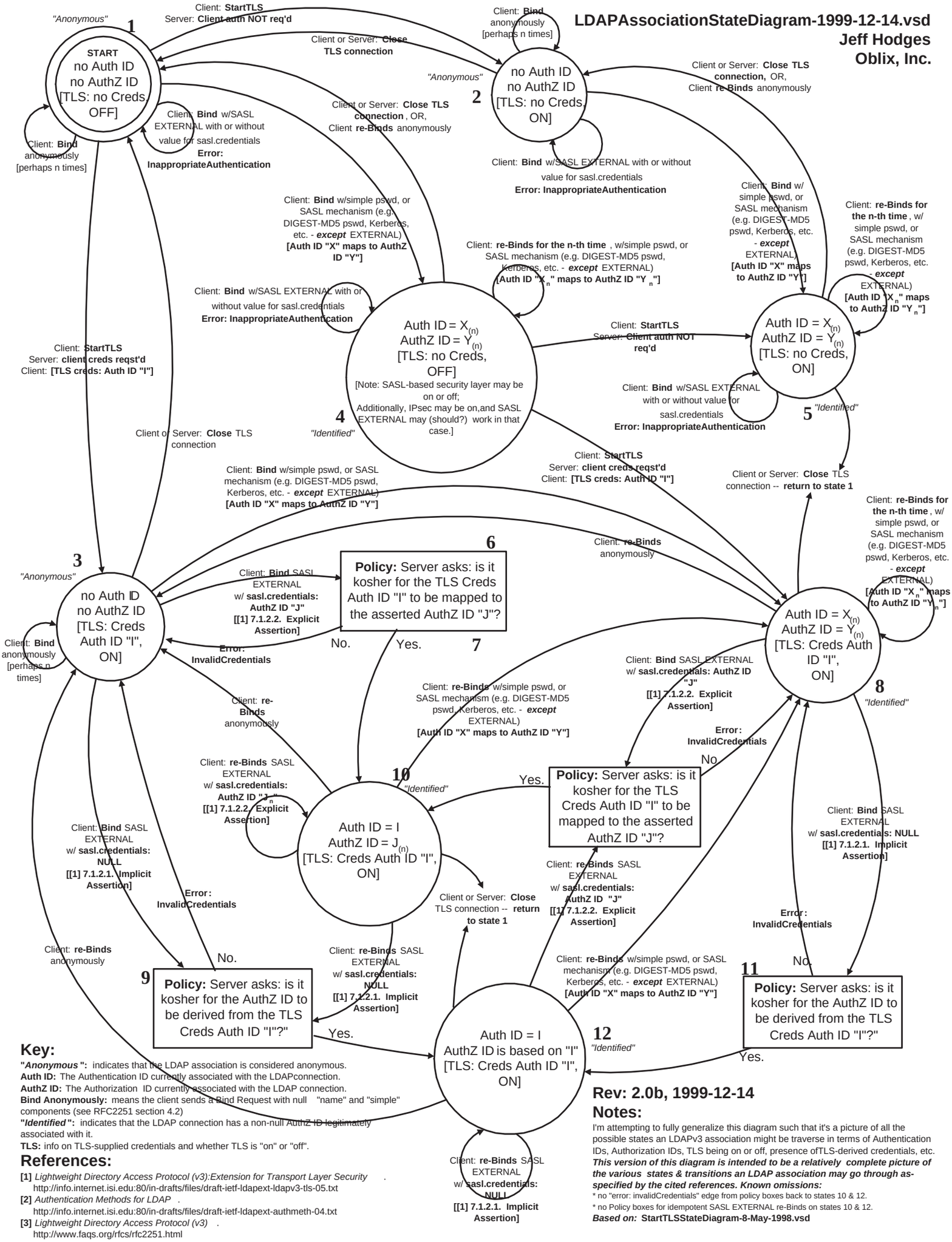
LDAPAssociationStateDiagram-1999-12-14.vsd

Jeff Hodges
Oblix, Inc.



Key:

"*Anonymous*": indicates that the LDAP association is considered anonymous.
Auth ID: The Authentication ID currently associated with the LDAPconnection.
AuthZ ID: The Authorization ID currently associated with the LDAP connection.
Bind Anonymously: means the client sends a Bind Request with null "name" and "simple" components (see RFC2251 section 4.2)
"*Identified*": indicates that the LDAP connection has a non-null AuthZ ID legitimately associated with it.
TLS: info on TLS-supplied credentials and whether TLS is "on" or "off".

References:

[1] *Lightweight Directory Access Protocol (v3):Extension for Transport Layer Security* .
http://info.internet.isi.edu:80/in-drafts/files/draft-ietf-ldapext-ldapv3-tls-05.txt
[2] *Authentication Methods for LDAP* .
http://info.internet.isi.edu:80/in-drafts/files/draft-ietf-ldapext-authmeth-04.txt
[3] *Lightweight Directory Access Protocol (v3)* .
http://www.faqs.org/rfcs/rfc2251.html

Rev: 2.0b, 1999-12-14

Notes:

I'm attempting to fully generalize this diagram such that it's a picture of all the possible states an LDAPv3 association might be traverse in terms of Authentication IDs, Authorization IDs, TLS being on or off, presence ofTLS-derived credentials, etc.
This version of this diagram is intended to be a relatively complete picture of the various states & transitions an LDAP association may go through as-specified by the cited references. Known omissions:
* no "error: invalidCredentials" edge from policy boxes back to states 10 & 12.
* no Policy boxes for idempotent SASL EXTERNAL re-Binds on states 10 & 12.

Based on: **StartTLSStateDiagram-8-May-1998.vsd**