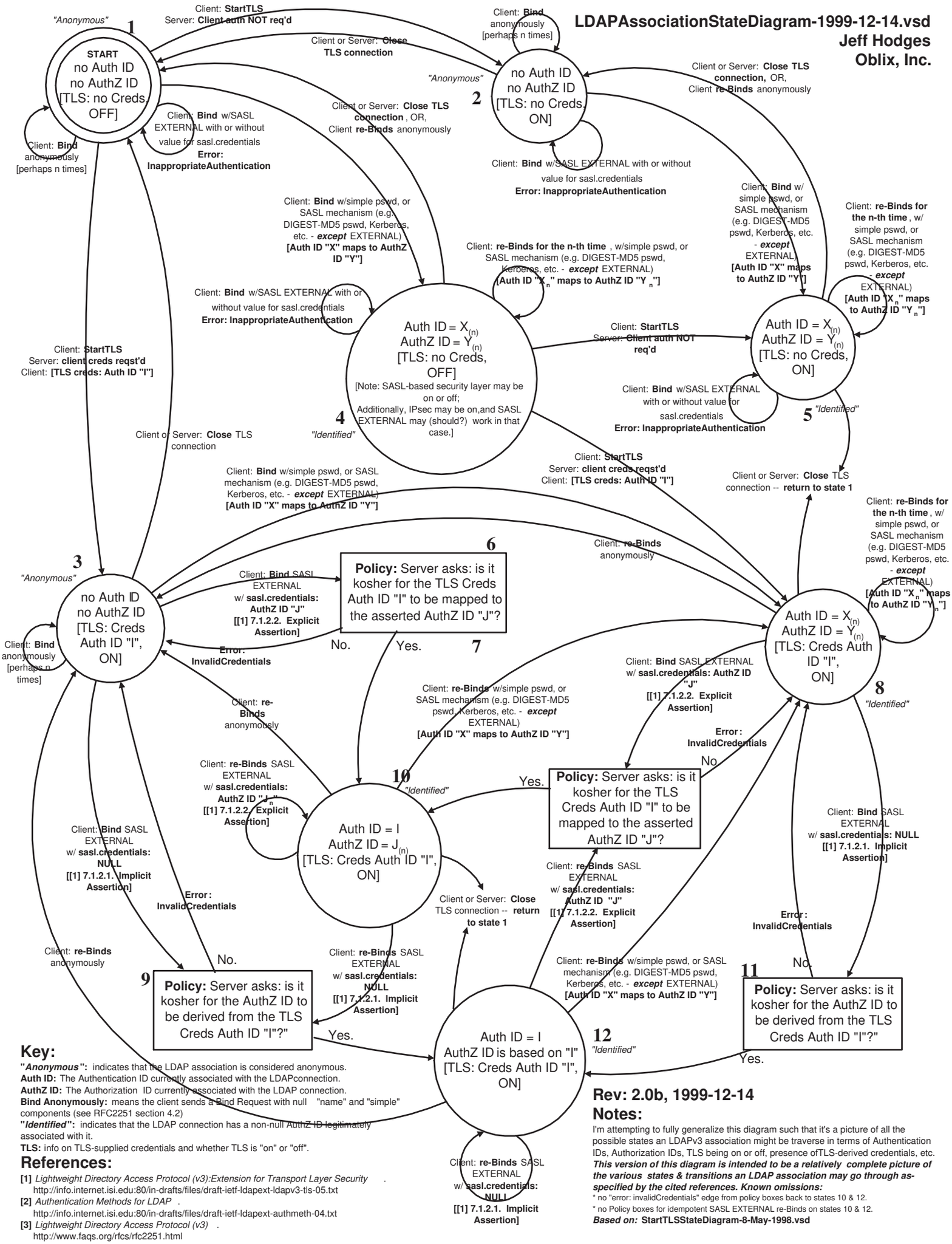
LDAPAssociationStateDiagram-1999-12-14.vsd
Jeff Hodges
Oblix, Inc.
"Anonymous"
1
START
no Auth ID
no AuthZ ID
[TLS: no Creds, OFF]
Client: StartTLS
Server: Client auth NOT req'd
Client or Server: Close TLS connection
Client: Bind anonymously [perhaps n times]
Client: Bind w/SASL EXTERNAL with or without value for sasl.credentials
Error: InappropriateAuthentication
Client or Server: Close TLS connection , OR, Client re-Binds anonymously
"Anonymous"
2
no Auth ID
no AuthZ ID
[TLS: no Creds, ON]
Client: Bind anonymously [perhaps n times]
Client or Server: Close TLS connection, OR, Client re-Binds anonymously
Client: Bind w/SASL EXTERNAL with or without value for sasl.credentials
Error: InappropriateAuthentication
Client: Bind w/simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X" maps to AuthZ ID "Y"]
Client: re-Binds for the n-th time , w/simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X_n" maps to AuthZ ID "Y_n"]
Client: Bind w/ simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X" maps to AuthZ ID "Y"]
Client: re-Binds for the n-th time , w/ simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X_n" maps to AuthZ ID "Y_n"]
Client: Bind w/SASL EXTERNAL with or without value for sasl.credentials
Error: InappropriateAuthentication
Auth ID = X(n)
AuthZ ID = Y(n)
[TLS: no Creds, OFF]
[Note: SASL-based security layer may be on or off;
Additionally, IPsec may be on,and SASL EXTERNAL may (should?) work in that case.]
4
"Identified"
Client: StartTLS
Server: Client auth NOT req'd
Auth ID = X(n)
AuthZ ID = Y(n)
[TLS: no Creds, ON]
Client: Bind w/SASL EXTERNAL with or without value for sasl.credentials
Error: InappropriateAuthentication
5
"Identified"
Client: StartTLS
Server: client creds reqst'd
Client: [TLS creds: Auth ID "I"]
Client or Server: Close TLS connection
Client: Bind w/simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X" maps to AuthZ ID "Y"]
Client: StartTLS
Server: client creds reqst'd
Client: [TLS creds: Auth ID "I"]
Client or Server: Close TLS connection -- return to state 1
3
"Anonymous"
no Auth ID
no AuthZ ID
[TLS: Creds Auth ID "I", ON]
Client: Bind anonymously [perhaps n times]
6
Policy: Server asks: is it kosher for the TLS Creds Auth ID "I" to be mapped to the asserted AuthZ ID "J"?
Client: Bind SASL EXTERNAL w/ sasl.credentials: AuthZ ID "J" [[1] 7.1.2.2. Explicit Assertion]
No.
Yes.
7
Error: InvalidCredentials
Client: re-Binds anonymously
Client: re-Binds anonymously
Auth ID = X(n)
AuthZ ID = Y(n)
[TLS: Creds Auth ID "I", ON]
Client: re-Binds for the n-th time , w/ simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X_n" maps to AuthZ ID "Y_n"]
8
"Identified"
Client: Bind SASL EXTERNAL w/ sasl.credentials: AuthZ ID "J" [[1] 7.1.2.2. Explicit Assertion]
Client: re-Binds w/simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X" maps to AuthZ ID "Y"]
Error: InvalidCredentials
No
Yes.
Policy: Server asks: is it kosher for the TLS Creds Auth ID "I" to be mapped to the asserted AuthZ ID "J"?
10
"Identified"
Client: re-Binds SASL EXTERNAL w/ sasl.credentials: AuthZ ID "J_n" [[1] 7.1.2.2. Explicit Assertion]
Auth ID = I
AuthZ ID = J(n)
[TLS: Creds Auth ID "I", ON]
Client: Bind SASL EXTERNAL w/ sasl.credentials: NULL [[1] 7.1.2.1. Implicit Assertion]
Client: re-Binds SASL EXTERNAL w/ sasl.credentials: AuthZ ID "J" [[1] 7.1.2.2. Explicit Assertion]
Client: Bind SASL EXTERNAL w/ sasl.credentials: NULL [[1] 7.1.2.1. Implicit Assertion]
Error: InvalidCredentials
Client or Server: Close TLS connection -- return to state 1
Error: InvalidCredentials
Client: re-Binds anonymously
No.
9
Policy: Server asks: is it kosher for the AuthZ ID to be derived from the TLS Creds Auth ID "I"?
Client: re-Binds SASL EXTERNAL w/ sasl.credentials: NULL [[1] 7.1.2.1. Implicit Assertion]
Client: re-Binds w/simple pswd, or SASL mechanism (e.g. DIGEST-MD5 pswd, Kerberos, etc. - except EXTERNAL)
[Auth ID "X" maps to AuthZ ID "Y"]
No.
11
Policy: Server asks: is it kosher for the AuthZ ID to be derived from the TLS Creds Auth ID "I"?
Yes.
Yes.
Auth ID = I
AuthZ ID is based on "I"
[TLS: Creds Auth ID "I", ON]
12
"Identified"
Client: re-Binds SASL EXTERNAL w/ sasl.credentials: NULL [[1] 7.1.2.1. Implicit Assertion]
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