How to enable LDAP over SSL using the Virginia Tech’s Open-SSL Certificate Authority
By: Scott Cassell, Systems Architect, VTMig, Virginia Tech
FEBRUARY 2002 V1.01

The network traffic generated by the Lightweight Directory Access Protocol (LDAP) is by default unsecured. Often the sensitive nature of the data obtained by an LDAP client dictates that a secure channel be used. To accomplish this LDAP over SSL can be implemented. This document details the steps required to implement LDAP-SSL using a non-Microsoft certificate authority. The standard port for LDAP is 389 and 636 for LDAP-SSL.

To prepare a domain controller to communicate using LDAP-SSL, perform the following steps.

- Download the root certificate from the Virginia Tech’s OpenSSL CA web site (currently http://box177.cc.vt.edu/htdocs-public).
- On the domain controller, open MMC and add the certificates snap-in.
- First, add the certificates snap-in for the “computer account (local computer)” and then the “my user account”. You will use the computer account to import the certificates you need for LDAP-SSL. If you have problems during testing you may use the “my user account” MMC to remove any personal certificates to ensure they are not creating the problem.
- Within the local computer certificates MMC right click trusted root certification authorities, and select “all tasks” and then “import”.

At this point you should complete the import wizard and verify that the certificate from the Virginia Tech CA is in the list of certificates under the trusted root certification authorities. All certificates imported for LDAP-SSL must be in the DER format. The format of the certificate is controlled by the issuer (the Virginia Tech CA in this case).

At this point the domain controller trusts the Virginia Tech Certificate Authority. Verify that the root certificate is listed in the trusted root certification authorities. To view the certificates properties you can double click on its name in the list. Now that the domain controller has the root certificate you should complete the same steps on the client computer that will use LDAP-SSL to connect to the domain controller.

The next step will be done on the domain controller. You must generate a request for an application-style server (as apposed to a web server) certificate. A tool that may be used to generate the request may be can be found at http://www.w2k.vt.edu/tools/getcert.htm. When you run this tool you must select the option “use local machine store”. A properly completed certificate request is listed next. In this example the data coded in the “identifying information” fields includes standardized data for Virginia Tech Certificates.
Please note the "Usage OID" field. You must manually add the last 1 to this field. The object ID must be 1.3.6.1.5.5.7.3.1. This data will be returned in the certificate that is sent back as an "enhanced key usage" extension.

The Common Name (CN) of this certificate request must match the FQDN of the domain controller. Another method is to have the DNS entry in the subject alternative name extension be the FQDN on the domain controller. However the certificate request tool that is mentioned previously does not allow for setting this field.
Store the certificate request on the hard drive and then upload it to the Virginia Tech CA for signing. Remember that all certificates used for LDAP-SSL must be in the DER format. The format of the returned certificate is controlled by the issuer. Each domain controller that is to utilize LDAP-SSL must be setup in similar fashion as outline previously. This includes child domain controllers.

Once the certificate has been signed, download it to the domain controller. You will use the certificates (local computer) MMC to import this certificate into the personal store. Right click on personal and select “all tasks” and then “import”. After this certificate has been imported you can double click on it to check the properties. Using the properties page verify the following:

- On the general tab you see a statement that indicates “you have a private key that corresponds to this certificate”.
- The location of the certificate is the personal store of the local computer.
- That the name of the certificate is the FQDN of the domain controller.
- That the key usage allows for data encipherment.
- That the enhanced key usage is server authentication (1.3.6.1.5.5.7.3.1)

Sample screen shoots are included at the end of this document.

The windows 2000 resource kit comes with a utility, LDP.exe that will allow you to connect to the domain controller from a client. Start this tool, select connection and then connect. Type the FQDN of the domain controller and enter 636 in the port number.