SUN BLUEPRINTS APPROVED

Securing LDAP Through TLS/SSL—A Cookbook

By Steffo Weber

Sun BluePrints™ OnLine - June, 2002

`http://www.sun.com/blueprints`

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95045 U.S.A.
650 960-1300 fax 650 969-9131

Part No.: 816-5203-10
Revision 01, 06/10/02
Edition: June 2002

Copyright 2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.sun.com/patents and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, JavaScripts, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

Netscape is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun’s licensees who implement OPEN LOOK GUIs and otherwise comply with Sun’s written license agreements.

Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Sun Microsystems, Inc. license agreements and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1998), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuels relatants à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuels peuvent inclure un ou plus des brevets américains énumérés à http://www.sun.com/patents et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l’utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, parquelque moyen que ce soit, sans l’autorisation préalable et écrite de Sun et de ses bailleurs de licence, s’il y ena.ls

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l’Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d’autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d’autres pays.

Netscape et sont des marque de fabrique ou des marque déposées de Netscape Communications Corporation. aux Etats-Unis et dans d’autres pays.

L’interface d’utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développment du concept des interfaces d’utilisation visuelle ou graphique pour l’industrie de l’informatique. Sun détient une license non exclusive do Xerox sur l’interface d’utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l’interface d ’utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L’ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L’APTITUDE A UNE UTILISATION PARTICULIERE OU A L’ABSENCE DE CONTREFAÇON.

Please
Recycle

Adobe PostScript

Securing LDAP Through TLS/ SSL—A Cookbook

Deploying secure Lightweight Directory Access Protocol (LDAP) connections is becoming more demanding as companies choose to build up and maintain a central repository. This article details the steps on how to set up the Sun^{TM} Open Net Environment (Sun^{TM} ONE) and the Sun^{TM} ONE Directory Server software so that it can be accessed securely from command line tools (for example, `ldapadd`, `ldapmodify`, or `ldapsearch`). More precisely, this article describes how client and server authentication can be accomplished with the Sun ONE platform products. In this article, security is accomplished two ways:

- Transport Layer Security (TLS)/Secure Socket Layer (SSL) Protocol—which provides a mechanism for ensuring the integrity and confidentiality of the transferred data.
- Authentication based on SSL certificates—which is used to guarantee the identity of the data sources.

This cookbook has been tested with the following products and releases:

- Solaris^{TM} 8 Operating Environment (updates 07/01, 10/01, and 02/02). Be sure to install the latest patch cluster.
- Sun ONE Directory Server software (the document has been tested with versions 5.0 and 5.1)
- The Public Key Cryptographic Standard (PKCS#11) toolkit (the current version is `cpkg106.zip`)

If you do not have access to a certificate authority (CA) for getting an SSL client and server certificates, you can use the Sun^{TM} ONE Certificate Server software (or the publicly available `certutil` tool). This article uses the Sun ONE Certificate Server software.

The basic steps for securing LDAP with SSL using your own CA are:

1. Setting up the Directory Server and the Certificate Server (CS).

2. Generating an SSL server certificate.

3. Generating an SSL client certificate.
4. Setting up the appropriate trust-relations.
5. Enabling SSL for the Sun ONE Directory Server software.
6. Setting up LDAP/SSL server authentication.
7. Setting up LDAP/SSL client authentication.

For this article, it is assumed that you have a basic understanding of how certificate-based public-key-cryptography works. Because the certificates are bound to the owner's name, the fictional business of iNIT8 was created for this article. iNIT8 uses the Sun ONE Directory Server Console to set up secure LDAP connections.

Note – All iPlanet products have been rebranded as Sun ONE platform products.

Setting Up the Directory Server and the Certificate Server

You can install both the Sun ONE Directory Server software and the Sun ONE Certificate Server software on the same machine. In production environments, for security reasons, the Sun ONE Certificate Server software is installed on a different machine. The Sun ONE Certificate Server software comes bundled with its own directory server, which holds specific data and can reside on a separate machine depending on your deployment. For the sake of simplicity in this article, all three servers, Sun ONE Directory Server software, Sun ONE Certificate Server software, and the certificate server-specific directory server are installed on the same machine.

In our example, the installation parameters for the Sun ONE Certificate Server software and the bundled directory server are as follows:

```
Software: certificate-4.2-domestic-us.sparc-sun-solaris2.6.tar.gz

Install location: /opt/iplanet/server4
Directory Service Port: 400
Directory Administration Port: 4000
Computer Name: sunshine.init8.net
Directory Server Identifier: sunshine
Administrator ID: admin
Password: manager
Directory Manager: cn=Directory Manager
Password: dirmanager
Suffix: o=init8.net
```

Note – This installation procedure offers you the option to run the Sun ONE software servers under UID `nobody` and GID `nobody`. As an even better security practice, pick a unique user/group ID, for example, `ldap` or `cert`.

The Sun ONE Directory Server software has the following installation parameters:

```
Software: directory-5.1-us.sparc-sun-solaris2.8.tar.gz

Install location: /opt/iplanet/server5
Directory Service Port: 389
Directory Administration Port: 3890
Computer Name: sunshine.init8.net
Directory Server Identifier: sunshine
Administrator ID: admin
Password: manager
Directory Manager: cn=Directory Manager
Password: dirmanager
Suffix: o=iNIT8.net
```

Note – The suffix `o=init8.net` in the Sun ONE Directory Server software installation parameters is necessary. Do not use the `dc=init8`, `dc=net` suffix. It prevents the mapping defined in the section , "Setting Up LDAP/SSL Client Authentication" from working.

If you already have deployed a Certificate Server, you can skip this section.

Three certificates are needed for setting up a Certificate Authority (CA):

- CA certificate (freshly generated during setup) to sign SSL certificates
- SSL server certificate for the Certificate Server to communicate through the browser and SSL with the Certificate Server
- SSL client certificate for the Certificate Server administrator (CS administrator).

  The SSL client certificate is needed in order to authenticate yourself not only through username/password but by using a public-key method against the Certificate Server.

▼ To Set Up the Certificate Server

1. **Go to** `/opt/iplanet/server4` **and execute** `startconsole`**.**

2. **Connect to your host at** `http://sunshine.init8.net:4000` **with user ID** `admin` **and the password selected during the installation (for example,** `manager`**).**

   In `init8.net` you will see `sunshine.init8.net` and its group of three servers: Certificate Server (`cert-sunshine`), Administration Server, and Directory Server.

3. **Double-click the Certificate Server (**`cert-sunshine`**).**

   The Certificate Server realizes that this is your first access and automatically starts up an installation wizard. Do the following:

   a. **Create a new internal database:**

```
Instance ID: sunshine-db
Port Number: 38900
Directory Manager DN: cn=Directory Manager
Password: manager1
```

The wizard now creates a new internal database.

b. Add the following information about the administrator:

```
Administrator ID: admin
Full Name: iNIT 8 Certificate Management System Administrator
Password: manager1
```

c. Click Next.

4. **Select the subsystem by choosing the** `Certificate Manager`

   a. Answering `No` **to the question of whether you want to generate the issuance of Wireless Transportation Layer Security (wTLS) certificates.**

   b. Click Next.

   c. Answer `No` **to the question of whether you want the current subsystems to connect to a remote data recovery manager.**

   The system now configures the internal database.

5. **Select the range of certificates (for example, 0x1 to 0x200).**

6. **(Optional) Enable the Online Certificate Status Protocol (OSCP) service.**

7. **Select the ports Sun ONE Certificate Server software will use:**

```
SSL administration port:      8200
SSL agent port:               8100
SSL end entity port:            443
Non-SSL end-entity port:      80 (check enable)
```

8. **Create a self-signed CA certificate:**

```
Token: internal
Password: manager1
Key type: RSA
Key length: 1024 bits.
```

   The system initializes the token.

9. **Select SHA-1 as cryptographic hash algorithm.**

10. **Enter the values for the subject Distinguished Name (DN) components of the CA signing certificate.**

    This should be done according to your needs. For this example choose the following:

    ```
    CN= iNIT8 Certificate Manager
    OU= CERT
    O=  iNIT8
    L=  Hamburg
    ST= HAMBURG
    C=  DE
    ```

    Click Next.

11. **Choose a validity period (for example, two years).**

12. **Activate the following extensions:**

    ```
    CA (Basic Constraints)
    S/MIME CA (Netscape certificate type)
    SSL CA  (Netscape certificate type)
    Object-signing CA  (Netscape certificate type)
    Authority key identifier
    Subject key identifier
    Key usage
    ```

13. **Sign the SSL certificate with your CA signing certificate by choosing the corresponding option in the dialog window.**

14. **Choose an internal token and RSA, 1024 Bit. Click Next.**

15. **Select SHA-1 as hash algorithm. Click Next.**

16. **Enter the following values for the subject DN components:**

```
CN= sunshine.init8.net
OU= LDAP SSL
O=  iNIT8
L=  Hamburg
ST= HAMBURG
C=  DE
```

Click Next.

17. **Select a validity period.**

18. **Select the following extensions:**

```
SSL client (Netscape certificate type)
SSL server (Netscape certificate type)
Authority key identifier
Key usage
```

The wizard now generates the certificate.

19. **Select a single sign-on password (for example,** `manager1`**).**

The system now creates a single sign-on database.

20. **Follow the instructions and point your browser to** `https://sunshine.init8.net:8100` **to enroll as CS administrator Be sure to have JavaScript^{TM} technology enabled in your browser.**

The CS administrator role is used to approve certificate requests.

21. **Accept the server certificate.**

If you are not automatically directed to the enrollment page, go to `https://sunshine.init8.net:8100/ca/adminEnroll.html`. You are challenged with a form. Provide the following necessary information:

```
User ID: admin
Password: manager1

Full Name: iNIT8 CS administrator
Login Name: admin
E-Mail: csadmin@init8.net
Organizational Unit: iNIT8 CS
Organization: iNIT8
Country: DE

Validity: 1 year
Key length: 1024 Bit
```

Click Submit.

The Certificate Server now instructs your browser to generate a new key pair. If this is the first key pair to be generated in this browser, you are asked for a password to protect the Communicator's Certificate Database. The certificate database is a file which resides in `~/.netscape/cert.db7`. In order to protect this file, the data stored in the file is encrypted (this is similar to an encrypted SSH key file).

A new certificate is now displayed of which following is a partial example:

```
Certificate:
     Data:
       Version:  v3
       Serial Number: 0x4
       Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
       Issuer: CN=iNIT8 Certificate Manager, OU=CERT,
O=iNIT8,L=Hamburg, ST=HAMBURG,C=DE
       Validity:
         Not Before: Monday, December 17, 2001 9:43:40 PM
GMT+00:00
         Not  After: Tuesday, December 17, 2002 9:43:40 PM
GMT+00:00
       Subject: E=csadmin@init8.net,CN=iNIT8 CS
Administrator,UID=admin,OU=iNIT8 CS,O=iNIT8,C=DE
       Subject Public Key Info:
         Algorithm: RSA - 1.2.840.113549.1.1.1
         Public Key:
           Exponent: 65537
           Public Key Modulus: (1024 bits) :
           D6:B6:16:70:ED:89:BC:C5:4E:71:1D:BA:F0:04:81:48:
Extensions:
  Identifier: Netscape Certificate Type - 2.16.840.1.113730.1.1
    Critical: no
    Certificate Usage:
      SSL Client
  Identifier: Key Usage: - 2.5.29.15
    Critical: yes
    Key Usage:
      Digital Signature
      Non Repudiation
      Key Encipherment
(continued next page)
```

```
(continued from previous page)
  Identifier: Authority Key Identifier - 2.5.29.35
    Critical: no
    Key Identifier:

      04:34:FB:D9:41:55:36:8D:6D:C1:5A:73:A8:21:53:A8:
      F8:F2:C9:06
Signature:
  Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
  Signature:
    CA:7F:7A:2E:6C:29:9C:9A:CA:07:B1:27:27:26:A4:D1:
Base 64 encoded certificate
-----BEGIN CERTIFICATE-----
MIICvjCCAiegAwIBAgIBBDANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQGEwJERTEQ
-----END CERTIFICATE-----
```

22. **Check the certificate in the browser: Communicator→Tools→Security Info→Certificates→Yours.**

    This browser holds a certificate for iNIT8 CS Administrator's iNIT8 ID. If you try to verify the certificate, you will notice that it is not trusted, because the signing certificate, iNIT8 Certificate Manager, is not trusted (this certificate resides in the Signers class). See the section , “Setting Up the Appropriate Trust Relations” for details on how to modify the trust relationship using the shell tool `certutil`. You now have everything you need in order to apply and approve certificates for an SSL-secured LDAP transmission.

23. **Exit the Netscape™ console in the Sun ONE Certificate Server software directory `/opt/iplanet/server4`.**

Generating an SSL Server Certificate

In order to use SSL, you have to generate an SSL-LDAP server certificate.

▼ To Generate an SSL-LDAP Server Certificate

1. **Go to `/opt/iplanet/server5` and start the Sun ONE console.**

2. **Select `http://sunshine.init8.net:3890` as the administration URL and enter `admin/manager` as the username/password.**

3. **Double-click the Directory Server Icon (in the Server Group).**

   The Sun ONE Directory Server software Admin window opens.

4. **Select Manage Certificates from the Directory Server Admin window.**

5. **Select Security Device Password of the freshly installed Sun ONE Directory Server software.**

   a. **At the corresponding popup window, enter the password (for example, manager1).**

   b. **Click OK.**

6. **Request a new certificate by clicking Request and then click Request a certificate manually.**

   The wizard starts up.

7. **Enter the following information:**

```
Server name: sunshine.init8.net
Organization: iNIT8
Organizational Unit: directory@iNIT8
City: Hamburg
State: HAMBURG
Country: DE
```

   Click Next.

8. **Enter the password to access token (for example, `manager1`).**

9. **Select the place where the certificate request will be stored (choose either file or clipboard).**

   a. **Select File and save the request in `~/cert-request.txt`.**

b. **Click Done.**

You can then view the contents of the request using a UNIX shell. It will look like the following:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB1DCCAT0CAQAwgZMxCzAJBgNVBAYTAkRFMRAwDgYDVQQHEwdIYW1idXJnMQ4w
DAYDVQQKEwVpTklUODFFMEMGA1UECxw8AAAAZAAAAGkAAAByAAAAZQAAAGMAAAB0
AAAAbwAAAHIAAAB5AAAAQAAAAGkAAABOAAAASQAAAFQAAAA4MRswGQYDVQQDExJz
dW5zaGluZS5pbml0OC5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM2W
vARHmRUUevbOpV4bW/8bV8gxbnrx4uL359W/l9wEboUvZVkMrJlSfrXLMyqg1KNt
EFMYGxRwMCQzTiQ9KjUiE2HhuX5dvmq6+5VxJLXBDz5bpvBVF5ICW5IHtfNaIHrB
wPoLknbHiqqhJK6qejs5ly2DBsTR66E+N9yjOaqRAgMBAAGgADANBgkqhkiG9w0B
AQQFAAOBgQBO1OqhwuBKPc2Lc7bzJNc+iTQFBTuxdI3qnVQL2/iOuWYy7BJX1rNe
55iHaIrSzIRiYVRzHQW184IaX04tKBgs0RIgifD15QNYek4YTfGMIxIBKk5G3jD4
+yO8Bz3VblIlI0nvn9hr8LsnNns1Y+9X/A9xwJbcbff/f70yKVo6Vg==
 -----END NEW CERTIFICATE REQUEST-----
```

10. **Enter the request into the Sun ONE Certificate Server software.**

    a. **Point your browser to** `https://sunshine.init8.net:443` **and click SSL Server in the navigation frame.**

    b. **Copy the request from** `~/cert-request.txt` **and paste it into the PKCS#10 request area.**

Note – Sometimes the cut and paste option is unstable with the Netscape browser. If you experience any problems, open a new browser window and point it to `~/cert-request.txt` (for example, through `file:/cert-request.txt`). Then copy it through the Netscape browser's copy function and paste it into the PKCS#11 text field.

---

11. **Enter the LDAP server admin contact information (for example):**

```
Name: L. Dap
E-Mail: ldap@init8.net
Telephone: 040 123456
```

Click Submit.

12. **Approve the request by pointing your browser to** `https://sunshine.init8.net:8100/`.

13. **Look at the pending certificate requests. You can see the freshly generated PKCS#11 request. Approve it.**

    The Sun ONE Certificate Server software generates an SSL certificate which is presented to you. Sun ONE Certificate Server software shows you two `Base64` encoded certificates: a plain one and one in PKCS#7 format. Copy the plain one to the clipboard.

```
-----BEGIN CERTIFICATE-----
MIIC9TCCAl6gAwIBAgIBBTANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJERTEQ
MA4GA1UECBMHSEFNQlVSRzEQMA4GA1UEBxMHSGFtYnVyZzEOMAwGA1UEChMFaU5J
VDgxDTALBgNVBAsTBENFUlQxIjAgBgNVBAMTGWlOSVQ4IENlcnRpZmljYXRlIE1h
bmFnZXIwHhcNMDIwMTA4MTY0MzA2WhcNMDMwMTA4MTY0MzA2WjCBqTELMAkGA1UE
BhMCREUxEDAOBgNVBAgTB0hBTUJVUkcxEDAOBgNVBAcTB0hhbWJ1cmcxDjAMBgNV
BAoTBWlOSVQ4MUkwRwYDVQQLHEAAAABkAAAAaQAAAHIAAABlAAAAYwAAAHQAAABv
AAAAcgAAAHkAAABAAAAAaQAAAE4AAABJAAAAVAAAADgAAAAuMRswGQYDVQQDExJz
dW5zaGluZS5pbml0OC5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALP6
kj4H8GJyEItcbEKZrFWrCxzRhrnxtUPYAJGMcUUWgJHEkJmkvyOI3LhIUVCi/ctw
kKx7cYLIKrnVMhV2Ax9ruBqwG8YZ5htwFiDUDe4yg0c2CBnab80hjwdo2ef36o9n
Cb17ZaVlVzbLZQTGby3/wWdkuTG6QAglS+/VIU6RAgMBAAGjYTBfMBEGCWCGSAGG
+EIBAQQEAwIGQDAOBgNVHQ8BAf8EBAMCBPAwHwYDVR0jBBgwFoAUBDT72UFVNo1t
wVpzqCFTqPjyyQYwGQYDVR0RBBIwEIEObGRhcEBpbml0OC5uZXQwDQYJKoZIhvcN
AQEEBQADgYEAGr5zWzAD+dRZWrFy55PB80lyaH9jnlDlfpNnJgrEKL+HRulwrRt9
3Q1oGbo9NjoMt9XHLkchzvjnavJZE7z4hsFAwJnMUHkqdsa8wreBSrsR2HTi3ZJG
opxvWArFo7HDxZ6n9Di9SJlNkRhdceKWNpkXDmdSIfRuSQodrUlj36k=
-----END CERTIFICATE-----
```

14. **Install the certificate in your Sun ONE Directory Server software using the Sun ONE Directory Server software Certificate Wizard, and select Install.**

    a. **Paste it from the clipboard in the text box. If that doesn't work for you, try to save it in a file first and then point the wizard to the file.**

    b. **Click Next and the wizard shows you certificate information.**

15. **Click Next twice.**

16. **Enter the password for the database (for example, manager1). Click Done.**

    The certificate is now in the wizard's Manage Certificates window.

17. **Close the window.**

Generating an SSL Client Certificate

In order to use SSL, you also have to create an SSL-LDAP client certificate that can be used by `ldapsearch`.

Note – To complete this step you must have access to the `certutil` tool. You can download this tool from the Mozilla software or the Netscape™ software website at: `http://www.mozilla.org/projects/security/pki/nss/tools/` or `http://developer.netscape.com/software/tools/pkcs/up106.html`

▼ To Generate an SSL Client Certificate

For use with the command line tools like `ldapsearch`, `ldapadd`, etc., follow these steps:

1. **Generate a Netscape browser certificate.**

   a. **Point the browser at the Sun ONE Certificate Server software URL.**

   In this example case this is `https://sunshine.init8.net:443`.

b. Provide all necessary information.

```
Full Name: LDAP Client
User ID: steffo
Email Address: steffo@init8.net
Organization Unit: People
Organization: init8.net
```

Your browser should support the `KEYGEN` tag. This tag enables the browser to generate a keypair and send the public part to the Sun ONE Certificate Server software. The Sun ONE Certificate Server software then signs the key together with the additional information you provided.

When you have successfully applied for the certificate, Sun ONE Certificate Server software gives you a request ID under which your request is being processed. If your request has been approved by the CS Administrator, you have to import the certificate into your browser.

2. **Point your browser to** `http://sunshine.init8.net` **and click Retrieval.**

3. **Enter the request ID.**

   The signed certificate is presented to you.

4. **Scroll down the page and click Import your certificate.**

   You now have a new private key, stored in `~/.netscape/key.db` and a new certificate, stored in `~/.netscape/cert7.db`.

5. **From the Netscape browser check (Communicator→Tools→Security Info→Certificates→Yours) to verify that this procedure was successful.**

   A certificate called LDAP Client's iNIT8 ID should be present. Alternatively, you can use the `certutil`:

```
bash-2.03# ./certutil -L -d /.netscape | grep LDAP
LDAP Client's iNIT8 ID              u,u,u

bash-2.03# ./certutil -L -d /.netscape -n "LDAP Client's iNIT8 ID"
Certificate:
     Data:
       Version: 3 (0x2)
       Serial Number: 6 (0x6)
       Signature Algorithm: PKCS #1 MD5 With RSA Encryption
       Issuer: CN=iNIT8 Certificate Manager, OU=CERT,
       O=iNIT8, L=Hamburg, ST=HAMBURG, C=DE
“(“...)
```

6. **Extract the certificate, stored in `~/.netscape/cert7.db` to use with `ldapsearch`, `ldapadd`, etc. by using the program `certutil` from the PKCS#11 toolkit.**

```
bash-2.03# ./certutil -L -d /.netscape -n "LDAP Client's iNIT 8
ID"  -r > ~/certs/ldap-client.bin
```

Setting Up the Appropriate Trust Relations

Before you can use `ldapsearch` with SSL, make sure that the certificate of the CA that signed your SSL-client certificate is trusted.

Note – To complete this step you must have access to the `certutil` tool. You can download this tool from the Mozilla software or the Netscape™ software website at: `http://www.mozilla.org/projects/security/pki/nss/tools/` or `http://developer.netscape.com/software/tools/pkcs/up106.html`

▼ To Set Up the Appropriate Trust Relations

1. **Do this by running `certutil` or by viewing the certificate status from within the Netscape browser at Communicator→Tools→Security Info→Certificates→ Yours→<Certificate>→Verify.**

   You either get a box showing "The certificate has been successfully verified" or a negative message (for example, "Verification of the selected certificate failed for the following reasons: Certificate not trusted").

   The only crucial certificate is that of the CA who signed the certificate for the LDAP/SSL Server. The CA that must be trusted is the one that was set up in the section , "Setting Up the Directory Server and the Certificate Server." The corresponding certificate can be identified by its nickname iNIT8 Certificate Manager. The output of the corresponding `certutil -L` command should look like this:

   ```
   iNIT8 Certificate Manager - iNIT8   C,C,C
   ```

2. **This certificate is present in the `~/.netscape/cert7.db` file.**

   - If it is not in this file import by pointing your browser at `https://sunshine.init8.net:443` or by using the browser's import function if this certificate is not present in the `~/.netscape/cert7.db` file.

- If it resides in `~/.netscape/cert7.db` file but without the proper trust attributes change the certificate through:

```
bash-2.03# certutil -d /.netscape -n "iNIT8 Certificate Manager -
iNIT8"  -M -t "C,C,C"
```

Enabling SSL for the Sun ONE Directory Server Software

▼ To Enable SSL for LDAP Queries

1. **Double-click the Sun ONE Directory Server software (in this example it is named sunshine).**

   The Sun ONE Directory Server software interface shows up.

2. **Select Configuration.**

3. **Select Encryption.**

4. **Check Enable SSL for this server.**

5. **Choose RSA cipher family by clicking the corresponding checkbox.**

6. **Select a certificate.**

   If there is no certificate to select, something went wrong while installing the SSL server certificate. If this happens, check the file permissions.

7. **Set 636 as the default LDAP/SSL (LDAPS) port.**

8. **Enable Do not allow client authentication in a first step.**

Note – Do not restart the server from the Sun ONE console but from the Solaris OE shell, in order to avoid password file problems.

---

9. **Restart the server in order to start the LDAP/SSL (LDAPS) service.**

```
bash-2.03# pwd
/opt/iplanet/server5/slapd-sunshine
bash-2.03# ./stop-slapd
bash-2.03# ./start-slapd
Enter PIN for Internal (Software) Token: manager1
```

Setting Up LDAP/SSL Server Authentication

The standard Solaris OE LDAP command-line interface (CLI) tools do not allow access to the LDAP server through SSL. A modified version of the CLI tools come with Sun ONE Directory Server software and are located in `$LDAPHOME/shared/bin` (in this example, where LDAPHOME is `/opt/iplanet/server5`).

▼ To Set Up LDAP/SSL Server Authentication

1. **Check to see whether you can access the LDAP server in the usual way:**

```
bash-2.03# /usr/bin/ldapsearch -h sunshine.init8.net -p 389 -b
"o=init8.net" "cn=*"

cn=Directory Administrators, o=init8.net
objectClass=top
objectClass=groupofuniquenames
cn=Directory Administrators
```

Before trying the version in `$LDAPHOME/shared/bin,` make sure that the libraries under `$LDAPHOME/shared/lib` are added to `LD_LIBRARY_PATH` (for example, through `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/iplanet/server5/lib`).

2. **Try the version in `$LDAPHOME/shared/bin` without encryption:**

```
bash-2.03# /opt/iplanet/server5/shared/bin/ldapsearch -h
sunshine.init8.net -p 389 -b "o=init8.net"  "cn=*"


version: 1
dn: cn=Directory Administrators, o=init8.net
objectClass: top
objectClass: groupofuniquenames
cn: Directory Administrators
```

3. **To use SSL, you have to call `ldapsearch` with the `-Z` option. You can also use the following options:**

```
-p: SSL port
-K: Private key file
-P: Certificate database's file and pathname
-N: Certificate name
-W: Password of the private key file
```

A typical command looks like:

```
bash-2.03# /opt/iplanet/server5/shared/bin/ldapsearch -h
sunshine.init8.net -p 636 -Z -P /.netscape/cert7.db -b
"o=init8.net" "cn=*"
```

Note – This typical command does not perform client authentication.

Setting Up LDAP/SSL Client Authentication

Client authentication is desirable if you want to make sure that only authorized clients can access the directory server. There are two authentication steps:

- SSL client authentication
- LDAP BIND authentication

For SSL client authentication, the LDAP server checks the validity of the certificate presented by the client. If the SSL client is successfully authenticated, an LDAP BIND operation is performed. The following credentials are accepted for this operation:

- BIND DN and BIND PASSWORD (through `ldapsearch` options `-D` and `-w`)
- SSL Certificate's subject DN without checking the certificate
- SSL Certificate's subject DN with checking the certificate

The following procedures describe how to perform password-based and certificate-based BIND operations together with SSL client authentication.

Performing SSL Client Authentication and Password-Based BIND Operation

Use the LDAP client certificate generated in the section , "Generating an SSL Server Certificate."

▼ To Perform SSL-Client Authentication

1. **Force the LDAP server to trust the CA that signed the client certificate (that is adding iNIT8 CA to the list of trusted certificate issuers).**

   a. **Double-click on the directory server** `sunshine.init8.net` **from the sun ONE console.**

   b. **Select Manage Certificates from the task list.**

   c. **Click CA Certs, in the wizard window.**

      You will see a list of valid CA certificates similar to the list in the Netscape browser. iNIT8 Certificate Manager's certificate is not yet present.

   d. **Obtain the certificate by contacting the Sun ONE Certificate Server software at** `https://sunshine.init8.net`

   e. **Go to "Retrieval".**

   f. **Select the Sun ONE Certificate Server software certificate (CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8, L=Hamburg, ST=HAMBURG, C=DE) and copy the Base64 encoding to the clipboard.**

g. **Select Install... from the certificate wizard and paste the Base64 text block into the text box.**

h. **Click Next twice. When asked for the intended purpose, select Accepting connections from clients.**

The certificate should now be present in the CA Cert list.

2. **Tell the LDAP server to accept/force client authentication.**

a. **Go to the Encryption window of the Sun ONE Directory Server software** `sunshine.init8.net`.

b. **Select Require client authentication, and save the settings.**

c. **Restart the server from the Solaris OE shell.**

d. **Perform SSL client authentication with LDAP BIND based on username/ password by issuing:**

```
bash-2.03# /opt/iplanet/server5/shared/bin/ldapsearch -h
sunshine.init8.net -p 636 -Z -N "LDAP Client's iNIT8 ID" -K  /
.netscape/key3.db -P /.netscape/cert7.db -D "cn=Directory Manager"
-w "dirmanager" -W manager1 -b "o=init8.net" "uid=*" -v


version: 1
dn: uid=EHobbit,ou=People, o=init8.net
dn: uid=LHelm,ou=People, o=init8.net
dn: uid=steffo,ou=People,o=init8.net
```

Note – The previous example assumes that there is a user with a DN `cn=Directory Manager`. If you do not have such a user, use another DN. Check the ACIs on the directory subtree, if the previous example fails.

Submitting a bind DN with a password is secure in the above example, since the transmission of the credentials is protected by the encryption mechanisms used during the SSL session.

Performing SSL Client Authentication and Certificate-based BIND Operation

It is assumed that you are able to get successfully authenticated by a password-based BIND operation and an SSL client authentication.

▼ To Use the SSL Client Certificate as Credentials Rather Than a Username/Password Pair For the LDAP BIND Operation

There are two options:

- Let the LDAP server grant or deny access based solely on the Subject entry of the SSL certificate.
- Let access be granted or denied by comparing the client's certificate, presented during the SSL session initialization, against a certificate which is stored in the client's LDAP entry stored in the directory.

In both cases, the server must be able to map the information stored in the Subject entry of the certificate to an LDAP entry. The mapping is defined in a file called `certmap.conf` that resides in:

```
$LDAPHOME/shared/config/certmap.conf
```

The `verifycert` parameter controls what options become active. In this example, the file contains the following entry:

```
certmap init8 CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8,
L=Hamburg, ST=HAMBURG, C=DE
init8:DNComps                     o
init8:FilterComps             uid
#init8:verifycert              on
#init8:CmapLdapAttr           certSubjectDN
#init8:library                <path_to_shared_lib_or_dll>
#init8:InitFn                     <Init function's name>
```

It is crucial that the string `CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8, L=Hamburg, ST=HAMBURG, C=DE` is identical to the issuer string of the certificate.

Note – You must restart the LDAP server after modifying `certmap.conf`.

For the following examples based on access being granted or denied by comparing the client's certificate against a certificate, the ACIs are modified for the `iNIT8-subtree` as follows:

- ACI for anonymous access is removed.

- ACI for a user uid=steffo,ou=People,o=init8.net is added:

```
(targetattr = "*")
(version 3.0;
acl "LDAP Client Access";
allow (all)
(userdn = "ldap:///uid=steffo,ou=People, o=init8.net")
;)
```

1. **Perform a BIND operation based solely on the Subject entry:**

```
bash-2.03# ./ldapsearch -h sunshine.init8.net -p 636 -Z -N "LDAP
Client's  iNIT8 ID" -K /.netscape/key3.db -P /.netscape/cert7.db
-W manager1 -b "o=init8.net" "cn=*"
version: 1
dn: cn=Directory Administrators, o=iNIT8
objectClass: top
objectClass: groupofuniquenames
cn: Directory Administrators
```

Note – A successful client authentication depends inherently on the certmap.conf. If you have a slightly different directory information tree, things can look different. Check $LDAPHOME/slapd-sunshine/log/errors and $LDAPHOME/slapd-sunshine/log/access for errors.

The corresponding entries in the access log look as follows:

```
[04/Apr/2002:14:35:04 -0100] conn=2 op=6 MOD dn="o=init8.net"

[04/Apr/2002:14:35:05 -0100] conn=2 op=6 RESULT err=0 tag=103
nentries=0 etime=1

[04/Apr/2002:14:35:11 -0100] conn=3 fd=33 slot=33 SSL connection
from 129.157.157.161 to 129.157.157.228

[04/Apr/2002:14:35:11 -0100] conn=3 SSL 128-bit RC4; client
E=steffo@init8.net, CN=LDAP Client, UID=steffo, OU=People,
O=iNIT8; issuer CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8,
L=Hamburg, ST=HAMBURG, C=DE

[04/Apr/2002:14:35:11 -0100] conn=3 SSL client bound as
uid=steffo,ou=People,o=init8.net

[04/Apr/2002:14:35:11 -0100] conn=3 op=0 BIND dn="" method=sasl
version=3 mech=EXTERNAL

[04/Apr/2002:14:35:11 -0100] conn=3 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn="uid=steffo,ou=People,o=init8.net"

[04/Apr/2002:14:35:11 -0100] conn=3 op=1 SRCH base="o=init8.net"
scope=2 filter="(cn=*)" attrs=ALL

[04/Apr/2002:14:35:11 -0100] conn=3 op=1 RESULT err=0 tag=101
nentries=6 etime=0

[04/Apr/2002:14:35:11 -0100] conn=3 op=2 UNBIND

[04/Apr/2002:14:35:11 -0100] conn=3 op=2 fd=33 closed - U1
```

Note – The `BIND DN` matches the subject of the certificate.

In order to perform an LDAP BIND operation that compares the certificates, the LDAP server must hold the client's certificate in which the public key is stored.

In this example, the user is called LDAP Client.

2. **From the Sun ONE console, add the attribute** `usercertificate` **to the user's entry (Sun ONE Console→Directory→Users→LDAP Client→Properties (right mouse button)→Advanced→Add Attribute).**

   The Add Attribute dialog opens.

3. **To make sure that the transportation mode of the** `usercertificate` **attribute is binary, in the Add Attribute dialog, select the subtype Binary.**

4. **After adding the attribute, you have to add an attribute value in the Property Editor window. Obtain the value from** `~/certs/ldap-client.bin` **(the file you generated in the section , "Generating an SSL Server Certificate") in the file selector box.**

   Test whether the certificate can be found by submitting the following LDAP query:

   ```
   bash-2.03# /opt/iplanet/server5/shared/bin/ldapsearch -h
   sunshine.init8.net -p 389 -b "o=init8.net" "cn=*"
   ```

   The output is:

   ```
   dn: uid=steffo,ou=People,o=init8.net mail:
   steffo@init8.net objectClass: top objectClass: person
   objectClass: organizationalPerson objectClass: inetorgperson
   givenName: LDAP cn: LDAP Client uid: steffo sn: Client
   usercertificate;binary::MIIC3TCCAkagAwIBAgIBDDANBgkqhkiG9w0BAQQF
     ADB0MQswCQYDVQQGEwJERTEQMA4GA1UECBMHSEFNQlVSRzEQMA4GA1UEBxMHSG
     FtYnVyZzEOMAwGA1UEChMFaU5JVDgxDTALBgNVBAsTBENFUlQxIjAgBgNVBAMT
     GWlOSVQ4IENlcnRpZmljYXRlIE1hbFnZXIwHhcNMDIwMTEzMTExNjI1WhcNMDM
     wMTEzMTExNjI1WjCBijELMAkGA1UEBhMCREUxDjAMBgNVBAoTBWlOSVQ4MRYwF
     AYDVQQLEw1TcGVjaWFsIFVzZXJzMRcwFQYKCZImiZPyLGQBARMHTENsaWVudDE
     UMBIGA1UEAxMLTERBUCBDbGllbnQxJDAiBgkqhkiG9w0BCQEWFWxkYXAtY2xpZ
     W50QGluaXQ4Lm5ldDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAqfgnYy3
     XbZfZWNSqEoazLADnsTT55y7q+8GocDrAhSj/XqUXfY0AoztAMA1WCKujE/
     bTllxjFvGiTn5zGxMy4d75kZIzk+MciPxP53RK++q6rIefzOjjGMqXh4qYwzMhW
     AyeRWy4x8UWfslsECikxZWu3UjlB+wmwqQ3EdV+1Y0CAwEAAaNoMGYwEQYJYIZ
     IAYb4QgEBBAQDAgWgMA4GA1UdDwEBwQEAwIF4DAfBgNVHSMEGDAWgBQENPvZQV
     U2jW3BWnOoIVOo+PLJBjAgBgNVHREEGTAXgRVsZGFwLWNsaWVudEBpbml0OC5u
     ZXQwDQYJKoZIhvcNAQEEBQADgYEANZeAlIYS3TqWOK8YvNNfY71zI5xElzolkd
     qHqz+cPOCX2pX98YVM1Snx85nKcSddEn67wSnJhhgwhf1KS8Og+4WVCUoepzCK
     x8ulajciZlqCvUX2OSasVLJ9UHjYbp4qu7sti21EtgkdCLGsKU0jVpHFswil7m
     ERpaiKq6Kgno=
   ```

5. **As in the previous example, map the Subject entry to an LDAP entry by using the file** `certmap.conf`**.**

6. **Then tell the server to compare the certificate presented during the establishment of the SSL session against the certificate stored in the user's LDAP entry. This is done by setting the `verfifycert` parameter to on.** The following example contains the content of the certmap.conf file.

```
certmap init8 CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8,
L=Hamburg, ST=HAMBURG, C=DE
init8:DNComps                     o
init8:FilterComps             uid
init8:verifycert               on
#init8:CmapLdapAttr           certSubjectDN
#init8:library                <path_to_shared_lib_or_dll>
#init8:InitFn                     <Init function's name>
```

Again, it is crucial that the string `CN=iNIT8 Certificate Manager, OU=CERT, O=iNIT8, L=Hamburg, ST=HAMBURG, C=DE` is identical to the issuer string of the certificate.

7. **Perform a BIND operation based on the certificate's Subject entry:**

```
bash-2.03# ./ldapsearch -h sunshine.init8.net  -p 636 -Z -N "LDAP
Client's  iNIT8 ID" -K /.netscape/key3.db -P /.netscape/cert7.db
-W manager1 -b "o=init8.net" "cn=*"
version: 1
dn: cn=Directory Administrators, o=init8.net
objectClass: top
objectClass: groupofuniquenames
cn: Directory Administrators
```

The server verifies the certificate and access is granted only after successful verification.

The access log looks as follows:

```
[04/Apr/2002:15:00:09 -0100] conn=1 fd=29 slot=29 SSL connection
from 129.157.157.161 to 129.157.157.228

[04/Apr/2002:15:00:09 -0100] conn=1 SSL 128-bit RC4; client
E=steffo@init8.net, CN=LDAP Client, UID=steffo, OU=People,
O=init8.net; issuer CN=iNIT8 Certificate Manager, OU=CERT,
O=iNIT8, L=Hamburg, ST=HAMBURG, C=DE

[04/Apr/2002:15:00:09 -0100] conn=1 SSL client bound as
uid=steffo,ou=People,o=init8.net

[04/Apr/2002:15:00:09 -0100] conn=1 op=0 BIND dn="" method=sasl
version=3 mech=EXTERNAL

[04/Apr/2002:15:00:09 -0100] conn=1 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn="uid=steffo,ou=People,o=init8.net"

[04/Apr/2002:15:00:09 -0100] conn=1 op=1 SRCH base="o=iNIT8"
scope=2 filter="(cn=*)" attrs=ALL

[04/Apr/2002:15:00:09 -0100] conn=1 op=1 RESULT err=0 tag=101
nentries=6 etime=0

[04/Apr/2002:15:00:09 -0100] conn=1 op=2 UNBIND

[04/Apr/2002:15:00:09 -0100] conn=1 op=2 fd=29 closed - U1
```

Successful and Secure Installation

This article detailed how to set up an SSL-enabled LDAP-server; explaining how to perform client and server authentication. User access to the Sun ONE Directory Server software cannot only be granted on the base of passwords but also on the base of SSL certificates.

The success and the security of an SSL-enabled LDAP deployment, however, depends on additional factors, which are beyond the scope of this article. These factors are:

- Passwords—In this article, passwords like *manager*, *dirmanager*, and *manager1* were used. Make sure that your LDAP-deployment follows a proper password policy.
- Certificates/Private-Public Keypairs—The confidentiality of the private key is crucial to the overall security.

  Make sure that your company has a proper framework for using cryptography, explaining which cryptographic algorithms and key-lengths should be used, where to store, and how to protect items like a public key, the policy for certificate revocation, legislative issues, and roles and responsibilities.

- Architectural issues—Deciding which Sun ONE software server should reside on which physical machine and how to achieve high-availability. What other security mechanisms (network security, host-based security, auditing, etc.) can help to protect the critical data stored in the LDAP repository.
- Workstation/Client security—Deciding what measurements can be taken to prevent the client (which might store a public-key on its disk drive) from getting compromised by a malicious code like a virus. Also raising the security awareness of the user.

The secure installation and operation of an LDAP-server does not only depend on the security mechanisms, but also on the policies backing these mechanisms.

About the Author

Dr. Steffo Weber is a member of Sun Professional Services Web Technology team in Germany. Steffo has over 12 years experience in UNIX and network computing. His topics include security and Internet/Intranet architectures.

He is currently working on highly available service infrastructures, which include directory, communication and security services.

Before joining Sun, he worked with debis IT Security Services, where he developed and reviewed IT security policies and architectures in the areas of finance, telecommunication and transportation. He also was one of the founding members of dCERT, a commercial CERT service.

Steffo studied computer science at the University of Bonn, Germany, and obtained his Ph.D. from the faculty of Mathematics and Computer Science at the University of Leipzig.

Acknowledgments

The author would like to recognize the following individuals for their contributions to this article:

Tom Bialaski, Enterprise Engineering, co-author of the Sun BluePrints book, *Solaris and LDAP Naming Services*.

Michael Haines, Sun ONE E-Commerce Solutions, co-author of the Sun BluePrints book, *Solaris and LDAP Naming Services*.

Stephan Hausman, Sun Professional Services specialist for the Sun ONE Directory Server.

Neil A. Wilson, Sun Professional Services for Enterprise Services.

Additional thanks to Dirk Wriedt, and Martyn Johnson for their comments and technical expertise.