



LinOTP Manual

© LSE Leading Security Experts GmbH

Version 1.3

Contents

1 Introduction	3
1.1 Glossary	3
1.2 System overview	3
2 Installation	6
2.1 Rollout system	6
2.2 RADIUS-Server	7
3 Configuration	8
3.1 Key generation	8
3.2 LDAP-Server	8
3.3 Enrollment system	10
3.4 RADIUS-Server	11
4 Usage	13
A Upgrade from LinOTP v1.0 to v1.1	16
B Error handling / FAQs	18
B.1 TLS problems	18
B.2 Settings in ldap.conf are not used by otpadm	18
C License texts	20

1 Introduction

LSE LinOTP is a linux backend that provides radius authentication with one time passwords (OTP).

This is the manual for the LSE LinOTP Enterprise-Edition. Nevertheless the chapters about the FreeRADIUS- (2.2 and 3.4) and the OpenLDAP-Server (3.2) will also work for the Community-Edition.

1.1 Glossary

HMAC-OTP (HMAC-Based One Time Password Algorithm) is an open standard for generating one time passwords. It is defined in RFC4226.

RADIUS (Remote Authentication Dial In User Service) is an open standard for authenticating users and it is defined in RFC2865. LinOTP enables you to authenticate users with Aladdin eTokenNG OTP against a completely linux based backend.

1.2 System overview

Components

LinOTP integrates with FreeRADIUS and OpenLDAP. The central component is the FreeRADIUS module (rlm_linotp) for authentication via HMAC-OTP. It uses the connector library (libotpdb) for accessing the ldap directory. The ldap directory holds the necessary attributes for each user. The LinOTP admin tool (otpadm) is used to initialize an eTokenNG OTP and to manage the corresponding attributes in the LDAP directory.

Workflow

The user authenticates with his username, a static password and the OTP value at a web site, a VPN client or whichever radius client. The radius client forwards the authentication credentials to the RADIUS-Server. The RADIUS-Server – in this case the LinOTP module – requests the HMAC-OTP value from the ldap directory for the user who is authenticating. The LinOTP module calculates the next OTP value and compares it to the value presented by the user. The RADIUS-Server responds to the authentication request accordingly.

License

The LinOTP components used at runtime (FreeRADIUS module and connector library) are under GNU General Public License (GPL) Version 2. The admin tool (otpadm) for initializing the eToken NG OTP, the documentation and scripts are to be licensed from the LSE Leading Security Experts GmbH.

Expandability

Based on GPLv2 you got the possibility to enhance the functionality of the FreeRADIUS module and to perform audits and code reviews on the software easily.

Security parameter

The security of an HMAC-OTP based setup is influenced by several parameters.

In the default configuration the following parameters are used:

- OTP is a 6-digit number. This is the recommended minimum length for HMAC-OTPs (RFC4226). Using the Aladdin eToken NG OTP this is the only possible length, since the display in the eToken NG OTP device has 6 digits.
- OTP PIN is an alphanumeric static password with a minimum length of 8 characters. The minimum length can be set using the admin tool (otpadm) with the parameter `--minlen`. We recommend not to use PINs shorter than 8 characters.
- Maximum number of failed requests. This value is per default set to 10 failed requests. After this number of failed requests the account in the LDAP directory will be locked. The number of failed requests can be set using the admin tool (otpadm) with the parameter `--maxfail`. This value can be configured for each user separately.

- HMAC-OTP synchronization window. The value defines, what counter deviation will be accepted by the FreeRADIUS module. The default value is set to 50. Thus an authentication will be successful if the eToken NG OTP is a maximum of 50 counter steps apart from the value stored in the LDAP directory.

Further recommendations for considerations of usability and security of the HMAC-OTP parameters can be found in RFC4226.

Protected storing of attributes

LinOTP protects the sensitive attributes by using a symmetric encryption for the OTP-Key and a cryptographic hash function for the OTP PIN.

The following algorithms are used.

$$\text{LinOtpPinEnc} = \text{SHA256}(\text{pin} || \text{LinOtpPinSeed})$$

$$\text{LinOtpKeyEnc} = \text{AES256} - \text{CBC}(\text{key}, \text{LinOtpKeyIV}, \text{otpkey})$$

LinOtpKeyIV and LinOtpPinSeed both have a size of 256 bits and are generated from the random source `/dev/random`.

2 Installation

2.1 Rollout system

The rollout system is used for initializing the eToken NG OTP and for managing the OTP attributes in the LDAP directory. For these tasks the LinOTP admin tool (otpadm) is used.

For initializing the eToken NG OTP the Aladdin Linux Middleware (PKI Client or also called Run Time Environment, RTE) and the libusb is needed. For information on how to install the Aladdin Linux Middleware please refer to the Aladdin documentation. The libusb is contained in all common Linux distributions as a package and can be installed easily.

Needed: Aladdin RTE 4.55 or 5.00¹

Needed: libusb0.1 (tested: 0.1.5, 0.1.8, 0.1.12)

Please install the shipped binary "otpadm" either in `/usr/local/bin` or in another directory contained in your PATH.

License file

The admin tool (otpadm) needs a valid LSE license file to run correctly. You are handed this license file when purchasing your license for LSE LinOTP. The license file is personalized and not transferable to other installations of organizations. Please copy the license file to `$HOME/.otpadm-license` or to `/etc/otpadm/license` if you want to use it system wide for all user.

¹Aladdin RTE 5.00 is required for eToken NG-OTP Java 72k.

2.2 RADIUS-Server

With the LinOTP FreeRADIUS module (rlm_linotp) the RADIUS-Server is used for authentication via OTP.

You are handed the FreeRADIUS module as source code. For installation you need gcc, make, libtool as well as the libraries libusb, libldap and libssl and the corresponding header files.

Needed: libssl (tested: OpenSSL 0.9.7e, 0.9.8e), libldap2 (tested: 2.1.30, 2.3.32), FreeRADIUS (tested: 1.1.0, 1.1.3, 1.1.6, 1.1.7).

On debian based systems you can install the needed packages as follows:

```
1 $ apt-get install gcc make libtool libusb-dev libldap2-dev \  
2   libssl-dev libz-dev
```

The FreeRADIUS module uses a connector library (libotpdb) for communicating with the LDAP directory. This library is also shipped as source code and needs to be installed prior to the FreeRADIUS module.

For installing change to the directory libotpdb and do the following:

```
1 $ make  
2 $ sudo make install
```

The library is installed to /usr/local per default. On some systems /usr/local/lib might not be contained in the search path of the linker. In this case please add the entry /usr/local/bin to the file /etc/ld.so.conf and run /sbin/ldconfig:

```
1 $ echo /usr/local/lib >> /etc/ld.so.conf  
2 $ ldconfig
```

Unpack the source of the FreeRADIUS (freeradius-1.1.7.tar.gz) and change into the directory:

```
1 $ tar -xvzf freeradius-1.1.7.tar.gz  
2 $ cd freeradius-1.1.7
```

copy the directory rlm_linotp to the sources of FreeRADIUS:

```
1 $ cp -r /path/to/rlm_linotp src/modules/rlm_linotp  
2 $ echo rlm_linotp >> src/modules/stable
```

Please compile and install the FreeRADIUS as described in the documentation of FreeRADIUS.

3 Configuration

3.1 Key generation

LinOTP stores the sensitive OTP parameter symmetrically encrypted in the database. You may generate the encryption key using the admin tool (otpadm):

```
1 $ otpadm genkey
2 01:00:028bdb58cf2cbd5f5fa0e19cc0f906a431df37ab7fdca809fb461c96b3768de
```

Please memorize this key or store it in a protected file. It will be needed for the further configuration steps.

3.2 LDAP-Server

A few steps need to be taken for the usage of the LinOtpAccount-schema. We assume that you already got a basic installation of the openLDAP slapd up and running.

Our examples are using the following values. Please adapt them to your needs:

```
1 BASEDN          dc=linotp,dc=com
2 LDAP_HOST       10.0.0.123
3 LDAP_ADMIN      cn=admin,dc=linotp,dc=com
4 LDAP_OTPBASE    ou=users,dc=linotp,dc=com
```

For the FreeRADIUS module please add a separate user with reduced access rights. In our examples we add the user `cn=radius-otp,dc=linotp,dc=com`. You can choose any name you want to.

```
1 $ ldapadd -x -W -h $LDAP_HOST -D $LDAP_ADMIN << END
2 dn: cn=radius-otp,$BASEDN
3 objectClass: simpleSecurityObject
4 objectClass: organizationalRole
5 cn: radius-otp
6 description: RADIUS OTP
```

```
7 userPassword: replaceMeXXX
8 END
```

You may either add a separate LDAP user for the OTP administration with the admin tool (otpadm) or use an already existing LDAP admin user. This user must have the necessary access rights to add the objectClass to the OTP users and to write the OTP attributes.

If you wish to, you may at this point add a test user, to reproduce the examples in this documentation:

```
1 $ ldapadd -x -W -h $LDAP_HOST -D $LDAP_ADMIN << END
2 dn: ou=users,dc=linotp,dc=com
3 ou: users
4 objectClass: organizationalUnit
5 dn: uid=testuser,ou=users,dc=linotp,dc=com
6 objectClass: posixAccount
7 objectClass: organizationalRole
8 cn: testuser
9 uid: testuser
10 uidNumber: 502
11 gidNumber: 502
12 description: RADIUS OTP testuser
13 homeDirectory: /home/testuser
14 userPassword: ghPW
15 END
```

Now you need to copy the shipped schema file `linotp.schema` to the schema directory of your OpenLDAP installation. Usually the directory is named `/etc/ldap/schema` or `/etc/openldap/schema`.

```
1 $ cp linotp.schema /etc/ldap/schema
```

Please edit the configuration file of the slapd daemon.
This file should be `/etc/ldap/slapd.conf`.

```
1 $ vim /etc/ldap/slapd.conf
```

Within this file find the section where the schema files are included using the "include" statements. At this point please add the line:

```
1 include /etc/ldap/schema/linotp.schema
```

Please assure that the schema "posixAccount" is defined and configured in your slapd configuration.

```
1 # Schema and objectClass definitions
2 include      /etc/ldap/schema/core.schema
3 include      /etc/ldap/schema/cosine.schema
4 include      /etc/ldap/schema/inetorgperson.schema
5 include      /etc/ldap/schema/nis.schema
6 include      /etc/ldap/schema/linotp.schema
```

Now you need to edit the access rights on the attributes of the object class "LinOtpAccount". This is a very important step. When the access rights are misconfigured unauthorized users might access the sensitive OTP parameters. Therefore please test the access definitions immediately. Add the following block at the right place in your slapd configuration:

```
1 access to attrs=@LinOtpAccount
2   by dn="cn=admin,dc=linotp,dc=com" write
3   by dn="cn=radius-otp,dc=linotp,dc=com" write
4   by * none
```

For security reasons the communication between the admin tool or the FreeRADIUS module and the LDAP server will only work encrypted via TLS. The slapd daemon needs to be configured accordingly.

Please activate the settings TLSCertificateFile, TLSCertificateKeyFile and TLSCACertificateFile within the file slapd.conf. You may either use self signed certificates or certificates signed by a certificate authority. You may now test the access to the LDAP server via TLS using ldapsearch:

```
1 $ ldapsearch -ZZ -h $LDAP_HOST -b $BASEDN "(objectClass=*)"
```

If you are experiencing problems at this point, please read appendix B.1 TLS problems.

3.3 Enrollment system

The admin tool (otpadm) may take configuration via a config file or via command line parameters.

otpadm reads the configuration file /etc/otpadm/otpadmrc and \$HOME/.otpadmrc. Within these files you may specify the parameters as follows:

```
1 $ cat $HOME/.otpadmrc
2 --host 10.0.0.123
3 --binddn cn=admin,dc=linotp,dc=com
4 --filter uid=%s,ou=users,dc=linotp,dc=com
5 --enckey 01:00:028bdb58cf2cbd5f5fa0e19cc...
```

You can view all available parameters by running the command `otpadm` with the option `--help`. All command line parameters can be used as parameters in the config file.

Please note: If you want to change ldap- or TLS-specific settings, please note the modified paths for the configuration files:

OpenLDAP configuration for otpadm:

`/etc/otpadm/openldap/ldap.conf`

OpenSSL configuration for otpadm:

`/etc/otpadm/ssl`

`/etc/otpadm/ssl/certs`

`/etc/otpadm/ssl/cert.pem`

`/etc/otpadm/ssl/lib/engines`

`/etc/otpadm/ssl/private`

3.4 RADIUS-Server

Finally please configure the FreeRADIUS module (`rlm_linotp`). Locate the configuration directory of your FreeRADIUS installation. Usually this directory is `/etc/raddb`, `/etc/freeradius` or `/usr/local/etc/raddb`.

Copy the file `linotp.conf` that is shipped with LinOTP to this directory:

```
1 $ cp linotp.conf /etc/freeradius/
```

Please assure that this file got restrictive access right like (0600 or `-rw-----`). Now edit `linotp.conf` to your needs. The necessary parameters are `ldaphost`, `binddn`, `bindpw`, `searchfilter` und `enckey`. A minimal configuration might look like this:

```
1 linotp {
2     ldaphost = 10.0.0.123
3     ldapport = 389
4     binddn = "cn=radius-otp,dc=linotp,dc=com"
5     bindpw = "replaceMeXXX"
6     searchfilter = "uid=%s,ou=users,dc=linotp,dc=com"
7     resync-window-size = 10
```

Chapter 3 Configuration

```
8   enckey = "01:00:028bdb58cf2cbd5f5fa0e19cc..."
9   }
```

Now you need to activate the `linotp` module by editing the file `radiusd.conf`. Add the following entries to the sections `modules` and `authenticate`:

```
1 modules {
2     ...
3     $INCLUDE ${confdir}/linotp.conf
4 }
```

```
1 authenticate {
2     ...
3     linotp
4     ...
5 }
```

You may now configure the `linotp` module to be the default method for authentication. Of course any other configurations and combinations are also possible. For this you need to edit the file `users` in the configuration directory of your FreeRADIUS installation:

```
1 DEFAULT Auth-Type = LinOTP
```

Congratulations! You are now done with the configuration. Please start the `slapd` daemon and test your configuration with the `radclient`. Of course this will only work after having added users with OTP attributes in your LDAP directory.

Please test your configuration like this:

```
1 $ echo "User-Name = testuser@LOCAL, User-Password = 9059210926920" | \
2   radclient -s -x 10.0.0.123 auth testing123
```

4 Usage

Add OTP user

This example assumes that an LDAP user with an object class `posixAccount` already exists.

```
1 $ otpadm init testuser
2 Enter PIN or <enter> to autogenerate:
3 Generated PIN '90592109'
4 uid=testuser,ou=users,dc=linotp,dc=com initialized successfully
```

Alternatively, `otpadm` can import an existing key. Currently Aladdin eToken PASS XML key format is supported:

```
1 $ otpadm --import-key etpass:/path/to/key.xml:000300000468 --no-init-token init testuser
2 Imported key 'etpass:/path/to/key.xml:000300000468' successfully.
3 Enter OTP PIN or <enter> to autogenerate:
4 Generated PIN '90592109'
5 uid=testuser,ou=users,dc=linotp,dc=com initialized successfully
```

Resynchronize OTP user

For resynchronization no physical access to the eToken is necessary. `otpadm` requests the current OTP value and will then identify the current position of the counter. The current counter position will be stored in the LDAP directory. For resynchronization call `otpadm` the following way:

```
1 $ otpadm resync testuser <limit> <otp>
2 $ otpadm resync testuser 100000 123123
```

Limit specifies the number of iterations `otpadm` tries to determine the counter position.

If you got physical access to the Token, you may also do a hard resynchronization. Just call `otpadm init`. Key, counter, fail count and max fail will be written anew.

Change PIN of OTP user

Using the "setpin" command the static password of the OTP user can be changed.

```
1 $ otpadm setpin testuser
2 Enter PIN or <enter> to autogenerate:
3 Generated PIN '17382716'
4 Setting PIN for 'uid=testuser,ou=users,dc=linotp,dc=com'
```

Lock and unlock OTP user

The locking function "disable" marks the user as being locked in the LDAP directory. The authentication requests are denied by the rlm_linotp with the status "locked".

```
1 $ otpadm disable testuser
2 Disabling 'uid=testuser,ou=users,dc=linotp,dc=com'
3 $ otpadm enable testuser
4 Enabling 'uid=testuser,ou=users,dc=linotp,dc=com'
```

Delete OTP user

Using the command "remove" you can remove the OTP attributes of a user in the LDAP directory. Only the OTP attributes are removed, not the user himself:

```
1 $ otpadm remove testuser
2 Removing 'uid=testuser,ou=users,dc=linotp,dc=com'
```

Automation

The admin tool (otpadm) also supports a non-interactive mode. All values that are usually requested interactively can also be passed using a file descriptor.

The corresponding parameters are

```
1 --key-fd <file-descriptor>
2 --otp-pin-fd <file-descriptor>
3 --token-pin-fd <file-descriptor>
```

```
1 $ otpadm --otp-pin-fd 3 --token-pin-fd 4 --key-fd 5 \  
2   init testuser \  
3     3< /path/to/otp-pin-file \  
4     4< /path/to/token-pin-file \  
5     5< /path/to/key-file
```

The only exception to the LDAP bind password (bindpw). This may be specified as command line parameter (`--bindpw <pass>`) or may be defined in the configuration file `otpadmrc`.

A Upgrade from LinOTP v1.0 to v1.1

The main enhancements from version 1.0 to version 1.1 of LinOTP are:

- enhanced LDAP schema
- new attributes for OTP-PIN and OTP-Key

We provide the tool `linotp-ldap-upgrade` to manage the change to the new schema and to add the new attributes easily.

Please follow these steps:

1. Install new schema definition

First stop the LDAP server. Copy the file `linotp.schema` from the LinOTP v1.1 install archive to the schema configuration path of your LDAP server and restart the LDAP server.

```
1 $ cp linotp-1.1/linotp.schema /etc/ldap/schema/linotp.schema
```

2. Generate encryption key

You can use `otpadm v1.1` to generate the encryption key. Please memorize the key or pipe it to a protected file as you need this key in a later step.

```
1 $ otpadm genkey
2 01:00:028bdb58cf2cbd5f5fa0e19cc0f906a431df37ab7fdca809fb461c96b3768de
```

3. Convert LDAP entries

For converting the LDAP entries please use the script `linotp-ldap-upgrade`¹.

The script copies the attributes `LinOtpKey` and `LinOtpPin` of each OTP user in the LDAP directory to the new attributes `LinOtpKeyEnc` and `LinOtpPinHash`. The new attributes are now coexisting to the old ones.

Run the script like this example:

```
1 $ linotp-ldap-upgrade --ldapuri ldap://ldapserver/
2   --ldapbase dc=linotp,dc=com
3   --binddn cn=admin,dc=linotp,dc=com upgrade
```

¹Unter Umständen müssen fehlende Perl-Module nachinstalliert werden, bevor das Script ausgeführt werden kann. Sämtliche benötigten Module finden Sie auf [CPAN](#).

This way you can use - with some restrictions - the old and the new version of the FreeRADIUS module at the same time. Please be aware of the following restrictions:

- If a new user is enrolled with `optadm v1.1` this user will only get the new attributes. Such a user will not be able to authenticate against a FreeRADIUS server which would still use the LinOTP module v1.0.
- If a PIN is changed using `otpadm v1.1` the new and the old PIN will be changed.
- If a PIN is changed using `otpadm v1.0` only the old PIN will be changed. Thus an administrator should always only use `otpadm v1.1`.
- At this point, the attributes are stored in the LDAP in the old and the new attributes, protected and unprotected. Therefore you should finalize the upgrade soon.

4. Upgrade of the FreeRADIUS module

Install the FreeRADIUS module version 1.1 on each RADIUS server.

Edit the file `linotp.conf` and add the parameter `enckey` with the encryption key you generated in the first step of this upgrade.

5. Finalize LDAP entries

This step should only be done after all RADIUS servers were upgraded to the LinOTP version 1.1.

Please run the perl script `linotp-ldap-upgrade` again. This time with the parameter *finalize*.

In this step the old unprotected attributes will be deleted from the LDAP server.

Please note: After this step old versions of the FreeRADIUS module (version 1.0) will not work anymore.

After running the migrations script, you finished the upgrade to version 1.1 successfully.

B Error handling / FAQs

B.1 TLS problems

The FreeRADIUS module and also the admin tool (otpadm) are using the TLS functions of libldap.

Per default libldap forces the verification of the certificate of the communication partner - in our case the LDAP server. If you do not have a correct installed CA certificate chain or if you are using self signed certificates it may happen that you can not connect to the LDAP server. You will be presented an error message like this:

```
1 ldap_start_tls_s failed: Connect error (-11)
2 additional info: error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:\
3 certificate verify failed
```

If your SSL certificate of your LDAP server was signed by a certificate authority you may introduce this CA certificate to libldap. Therefore you need to edit the file ldap.conf and add the following entry:

```
1 TLS_CACERT /path/to/cacert.pem
```

The FreeRADIUS module will use the system installation of the libldap. Therefore the correct configuration file will be \$HOME/.ldaprc and /usr/local/etc/openldap/ldap.conf. On some systems it will be /etc/ldap/ldap.conf or /etc/openldap/ldap.conf.

Please note: The admin tool (otpadm) uses another configuration file. Please also add the changes to /etc/otpadm/openldap/ldap.conf.

B.2 Settings in ldap.conf are not used by otpadm

The admin tool (otpadm) contains its own version of the LDAP and OpenSSL libraries. To avoid version conflicts these libraries are configured to look for their configuration files at runtime at another location.

Instead of the system wide pathes for OpenSSL and OpenLDAP the directories `/etc/otpadm/ssl` and `/etc/otpadm/openldap` are searched. Please take a look at the section for configuring `otpadm` for further information.

```
/etc/otpadm/ssl/  
/etc/otpadm/openldap/ldap.conf
```

C License texts

This product includes Software that was produced with the below licenses:

Copyright 1998–2007 The OpenLDAP Foundation
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998–2006 Kurt D. Zeilenga.
Portions Copyright 1998–2006 Net Boolean Incorporated.
Portions Copyright 2001–2006 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

Portions Copyright 1999–2005 Howard Y.H. Chu.
Portions Copyright 1999–2005 Symas Corporation.
Portions Copyright 1998–2003 Hallvard B. Furuseth.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided “as is” without express or implied warranty.

Portions Copyright (c) 1992–1996 Regents of the University of Michigan
. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty
.

The OpenLDAP Public License
Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions in source form must retain copyright statements and notices,
- 2.Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
- 3.Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ‘‘AS IS’’ AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED . IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999–2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Copyright (c) 1998–2007 The OpenSSL Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3.All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (C) 1995–1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3.All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-)
- 4.If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

SOFTWARE-LIZENZVERTRAG II

Die Module "LinOTP Konnektorbibliothek"/ "libotpdb" und "LinOTP FreeRADIUS-Plugin"/ "rlm_linotp" erhalten Sie unter den Bedingungen der nachfolgend reproduzierten Lizenz (GNU General Public License)

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights , we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights . These restrictions translate to certain responsibilities for you if you distribute copies of the software , or if you modify it .

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software , and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software .

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original , so that any problems introduced by others will not reflect on the original authors' reputations .

Finally , any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses , in effect making the program proprietary. To prevent this , we have made it clear that any patent must be licensed for everyone's free use or not licensed at all .

The precise terms and conditions for copying, distribution and modification follow .

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it , either verbatim or with modifications and/or translated into another

language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for

making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any

later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS