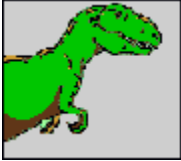# The Web Tool for Really Easy key and X.509 certificate management

### Web T-Rex Users Guide
### Version 1.2.15



**Lymeware Corporation**
**www.lymeware.com**

# Welcome to Web T-Rex

===========================================================

This web tool allows key and certificate maintenance using your favorite web browser.

It currently supports everything from key and certificate generation to revocation, display and validation.

If none of the above made any sense to you, then you may want to check out the FAQ (trex_faq.txt) and the **OpenSSL** project website ([www.openssl.org](www.openssl.org)) before going any further.

The following actions are available:

- **RSA Key Creation and maintenance utilities**
  Create, Modify format Display, or Verify a RSA Key pair of files.

- **Certificate Request Creation and maintenance utilities**
  Create, Modify format, Display, or Verify a Certificate Request (and optionally, a private RSA Key) file.

- **X.509 Certificate Creation and maintenance utilities**
  Create, Modify format, Display, or Verify a X.509 Certificate file (from a Certificate Request or CA Certificate).

  Create, Modify format, Display, or Verify a Certificate Authority (or Root or Self-Signed) X.509 Certificate file.

- **CRL (Certificate Revocation List) maintenance utilities**
  Create, Modify format, Display, or Verify a Certificate Revocation List file.

- **Miscellaneous Utilities**
  Additional maintenance, configuration, and troubleshooting utilities for the PKI system elements.

## Why Web T-Rex?

==========================================================

This product was built both because our company, Lymeware, needed a simple way to allow customers the ability to display and verify PKI components and because we kept seeing the same questions on that fine mailing list *openssl-users@openssl.org* and wanted to do our part to "cut through the noise".

Currently the Web T-Rex product is released and supported on two operating systems, Linux (on x86) and Cygwin (on win32 x86).  If you need it on something else, contact Lymeware for options.

## Linux Package Contents
==========================================================

This package comprises the Linux/x86 binary distribution of the Lymeware Web T-Rex product.  The Linux package was built on a Red Hat Linux 7.2 system on a i486 machine and consists of the following files in RPM package format:

```
./trex    - the tool itself,
./*.txt          - ASCII text documentation,
./*.rtf          - Raw Text Format (RTF)documentation,
./*.pdf          - AdobeTM Portable Document Format
                        (PDF) documentation,
./*.html         - HTML format documentation, and
./*.sh           - Bash shell script files,
```

## Linux Installation
==========================================================

The Web T-Rex product is distributed in a binary RPM file, and can be installed with the standard RPM install command:

```
rpm -i wtrex-1.2.15-i386.rpm
```

Web T-Rex is totally self-contained and requires no other packages to operate properly.

## Cygwin Package Contents
==========================================================

This package comprises the Win32/Cygwin binary distribution of the Lymeware Web T-Rex product.  The Cygwin package consists of the following files:

```
./trex.exe       - the tool itself,
```

```
./cygwin1.dll   - the only CygWin DLL needed,
./*.txt         - ASCII text documentation,
./*.rtf         - Raw Text Format (RTF)documentation,
./*.pdf         - AdobeTM Portable Document Format
                      (PDF) documentation, and
./*.sh          - Bash shell script files,
./*.bat         - MS-DOS batch files used to start the tool.
```

## Cygwin Installation
=======================================================================
The Web T-Rex product is distributed in a gzip-ed tar file, but can be unpacked with WinZip (www.winzip.com) or NetZip (www.netzip.com) and should be unpacked into its own directory (trex-n.n.n).  If you have Cygwin already installed then the only REQUIRED file is trex.exe and a configuration file (wtrex.conf by default), otherwise you need the single Cygwin dll file (usually something like **cygwin1.dll** and found in the **cygwin: the UNIX Emulation Engine** package).



## Web T-Rex Startup
=======================================================
The simplest method of starting Web T-Rex is in "unsecured" mode, since this mode does not require the certificates and keys that both the SSL mode and the TLS mode do.

From bash or another shell type:

**run.sh**

And you should see a sign-on screen like the following:

> Web T-Rex (with SSLv3/TLS 1.0 support) version N.N.N
> (Web Tool for Real Easy key and X.509 certificate management)
>     Copyright (c) 2000-2002 Lymeware Corporation, All Rights Reserved
>
>     Powered by the Lymeware NAC toolkit, version 1.4.3c
>     Copyright (c) 1999-2002 Lymeware Corporation
>
>     This product contains code from the OpenSSL Project
>     portions Copyright (c) 1998-2002 OpenSSL
>     This product contains code from the SSLeay Project
>     portions Copyright (c) 1998 Eric Young & Tim Hudson
>
>     Listening on port 8080

This means that the web server portion of the tool is up and waiting for requests from web browsers.

To access Web T-Rex with your web browser, the following URL address may be browsed (assuming the tool is running on a host with an IP address of 10.0.0.1):
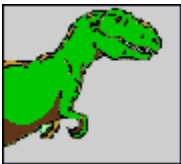
> http://10.0.0.1:8080/

If the browser is on the same host as the Web T-Rex:

> http://localhost:8080/

> or

> http://127.0.0.1:8080/



## Web T-Rex HTTP connection modes
========================================================

Web T-Rex supports three different HTTP connection modes (the way web browsers connect to the "web server" embedded in Web T-Rex):

• **"Insecure"** - standard HTTP, which transmits everything in cleartext,
• **"SSL"** - secure HTTP which transmits everything in an encrypted socket, and
• **"TLS"** - another secure HTTP, which transmits everything in a different, encrypted socket.

For more information on SSL and TLS, try www.google.com.

The default mode is **"insecure"** and is supported by all web browsers. It is STRONGLY suggested that the tool be used in **SSL** or **TLS** mode if being run over the Internet.



## Web T-Rex command line options
========================================================

The following command line options are available:

**trex -CCApath -cCAcert.pem [-d][-e][-fConfigfile] -kRSA_Key.pem [-p][-r]**
**-sServerCert.pem [-S][-T][-V][-v][-w]**

   **-CCApath = \*REQUIRED CA certificate path to hashed certificates**
   **-cCAcert = \*REQUIRED CA certificate (in PEM)**
   **-d = enable debug printing**
   **-e = enable WebCommand exit (disabled by default)**
   **-fConfigfile = define configuration file (wtrex.conf by default)**
   **-kRSA_Key = \*REQUIRED RSA Private key (in PEM)**
   **-p = display POST as HTML**
   **-r = print client/browser requests**
   **-S = force SSLv3 support**
   **-sServerCert = \*REQUIRED X.509 Server Cert (in PEM)**
   **-T = force TLS support (overrides SSLv3)**
   **-V = print version and exit**
   **-v = verbose printing**
   **-w = enable WebCommand weblog (disabled by default)**

**\*** required if "SSL" or "TLS" connection modes requested.
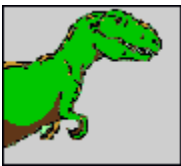

# Web T-Rex configuration file options

============================================================


# WebCommand™ support

============================================================

Web T-Rex (the NAC toolkit really) supports the notion of URL command words called WebCommands.  This allows the end user browser to send commands to the web tool without requiring specific links or form elements to be provided to the browser in HTML.

Web T-Rex can optionally provide support for two WebCommands: **exit** and **weblog**. These commands are "sent" in the URL.  For example, if the root URL is http://10.0.0.1:8080/ then the following URL would send the **exit** WebCommand (which if enabled, would cause the web tool to exit and end execution):

   http://10.0.0.1:8080/exit

The following command would display the current WebLog:

http://10.0.0.1:8080/weblog
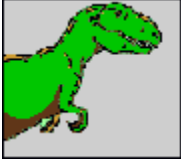
# WebLog™ HTML Access log support

============================================================

Web T-Rex (again, the NAC toolkit really) supports the concept of a HTML browse-able HTTP access log called a WebLog.  This allows end users to view access information without direct access (ssh/telnet/ftp/etc.) to the host machine.  While this option may be useful in secure internal network usage, it is not suggested for use on insure networks (the Internet).

# Web T-Rex Reference Platforms and Browser Information

============================================================

Web T-Rex has been built (and extensively tested) on:

•       Sun Solaris 7 & 8 SPARC machines, (not publicly available at this time)

•       Red Hat Linux 7.3 Intel x86 machines, and

•       Red Hat Cygwin 1.3.6-6 Intel x86 machines.

Web T-Rex has been tested with the following Web Browsers:
•       KDE konqueror 2.1 (Linux version)
•       Microsoft Internet Explorer 5.5 (Windows 9X/NT version)
•       Microsoft Internet Explorer 6.0 (Windows 9X/NT version)
•       Netscape 4.76 (SPARC/Solaris version)
•       Netscape 4.78 (Windows 9X/NT version)
•       Netscape 6.02 (Windows 9X/NT version)
•       Opera 5.0 (Windows 9X/NT version)
•       Opera 6.0 (Windows 9X/NT version)
•       Sun HotJava 3.0 (Solaris/Windows NT versions)

If you successfully test this with another web browser, please send your results to trex@lymeware.com and they will be added to the list.
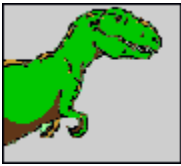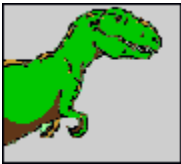
# Feedback

====================================================================

Any and all feedback, including bug reports, patches, virtual beer, and ideas, may be sent to trex@lymeware.com.

Any cool T-Rex (and other dinosaur) pictures can be sent to will@lymeware.com.



# References

====================================================================

IETF Request For Comments (RFC) Drafts

• RFC 1867 - Form-based File Upload in HTML, by E. Nebel, L. Masinter -November 1995

• RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, by N. Freed, N. Borenstein - November 1996

• RFC 2183 - Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field, by R. Troost, S. Dorner & K. Moore, Editor - August 1997

• RFC 2388 - Returning Values from Forms:  multipart/form-data, by L. Masinter - August 1998

• RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1, by R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee - June 1999

Other Documents

• Lymeware Network Appliance Core (NAC) Users Manual - by Lymeware Corporation - August 2000

• HTML 4.01 Specification - W3C Recommendation - 24 December 1999