

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 1/15

Purpose

The SSH feature is an optional module that provides encrypted communications between the APU102 console and a remote user. In addition, encrypted file transfers are provided.

When the SSH feature is enabled, Telnet connections are no longer available¹.

When a client connects to the SSH server running on the APU102, the initial handshake negotiates an encryption key unique to the session. The negotiation occurs in such a way that the “secrets” held by the server and the client are never exchanged over the communications channel.

SSH is similar in operation to HTTPS commonly used between web browsers and, for example, banking sites.

File Transfers Using ZMODEM
In the current version of the SSH feature, ZMODEM transfers used to send/receive file is not reliable. As an alternative, SCP is supported (and is easier to use than ZMODEM).

SSH Requirements

The SSH feature is supported only on the LX800 and T10 processor modules. The LPM-TX processor is not supported.

Features

When SSH is enabled, communications between the APU102 and a console user are encrypted using SSH (Secure Shell). SSH requires a compatible client (e.g. terminal program like PuTTY or TeraTerm).

¹ Telnet is available regardless of the department SSH setting when the unit is running NETMRS.

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 2/15

Disclaimer

Comet Electronics makes no guarantees whatsoever regarding the suitability or security of any third-party software such as WinSCP, PuTTY, or TeraTerm.

It is up to the user to establish that software is genuine, properly licensed, and compliant with any company Information Technology (IT) policies.

When in doubt, contact your IT for guidance.

File transfers can be made using SCP (Secure Copy), which operates over SSH.

Installation

Supported APU Software Updates

Only supported versions of the AEI application should be installed on units with the SSH update installed.

SSH relies on various programs that run during startup that older software updates may overwrite when installed.

Supported versions are: 5.1.1.132 and later; 5.2.0.15 and later.

Versions starting with 5.3 require the customer to perform the installation process. Version 5.3.5.2 and later already include this feature.

The supported versions include changes to exclude remote Telnet connections (when SSH is enabled) and additions to parameters that allow SSH and FTP to be enabled/disable.

The upgrade payload is large, so a fast and reliable link is required for remote installation.

1. Based on your board configuration (either LX800 or T10), update the following:

- LX800:
 - F.BAT
 - INSTSSH.EXE
 - ZIP.PSP
- T10:
 - F.BAT
 - SSHD_CONFIG

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 3/15

- o ZIP.PSP
- 2. Reboot APU to complete installation.

Once the updates are installed, the APU continues to accept Telnet and FTP connections as before.

Port Numbers

Typically, Telnet connections are accepted on TCP ports 23 and 1023. When communications occur over a cellular modem, the modem is often set to map an incoming port (e.g. 8001) to port 23 on a specific APU.

Cellular Modem

SSH communicates over port 22 so cellular modem settings need to be changed to pass external traffic to port 22.

FTP

Typically, the FTP server is used to collect AEI data available from external devices such as defect detectors.

To reduce the “attack surface” of the APU102, FTP should be disabled unless needed in a particular installation.

The updated AEI application (APU102.EXE) provides two new parameter settings accessed using the EP command:

- `Ports.ETHERNET.SSHEnable`
- `Ports.ETHERNET.FTPServerEnable`

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 4/15

Editing Ports.ETHERNET

Ctrl-B MOVES BACKWARDS AND Ctrl-U PRINTS HELP

```

IPAddress = 10.30.6.32 >
SubnetMask = 255.255.255.128 >
Gateway = >
DNSTableFilename = >
AlternateTelnetPortEnabled = 0 >
AlternateTelnetPort = 0 >
UseAlternateTelnetPortOnly = 0 >
DisableClientSideDNSCaching = 0 >
SshEnable = 1 >
FTPServerEnable = 1 >

```

Figure 1

When `SshEnable` is 0 (zero) when the APU starts, SSH is disabled; only Telnet connections will be accepted.

Setting `SshEnable` to 1 (one) will enable the SSH server at startup; only SSH connections will be accepted; Telnet connections will be refused.

The FTP server may be enabled/disabled by changing `FTPServerEnable` using the EP command. A setting of 0 (zero) disables the FTP server at startup; a setting of 1 (one) enables the FTP server at startup.

Initial SSH Connection

The client (terminal) program must be capable of SSH connections; Hyperterm will not work.

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH clients and servers each possess a unique identity certificate (the APU102's certificate is generated during initial installation). In some applications, these certificates are used by clients and servers to verify identities at the other end of a connection. This is analogous of the means used by web browsers to ensure that a banking site is genuine and not an impostor.

The first time an SSH client is used to connect to a server, the user will be prompted to accept the certificate (**Error! Reference source not found.**).

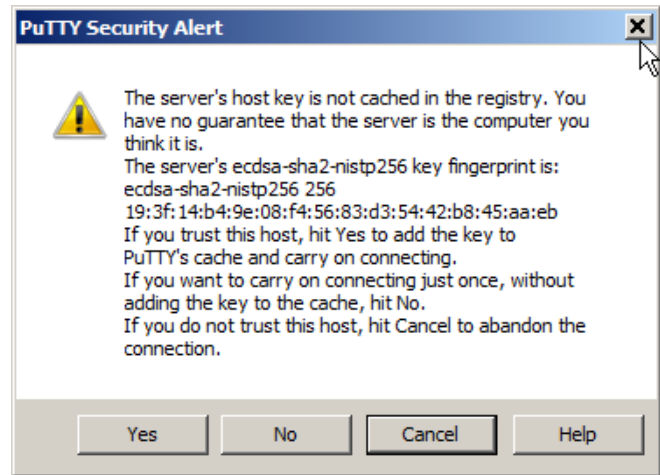


Figure 2

Once the connection is established (at this point, all communications between the APU102 and the client are encrypted), the user is prompted for a username and password (**Error! Reference source not found.**):

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 6/15

```

# login as: aei
# aei@10.30.6.32's password:
UNKNOWN

1. UNINITIALIZED
2. Inactive Session, Not Available for Selection
3. Inactive Session, Not Available for Selection
4. Inactive Session, Not Available for Selection
5. Log Off

Select the Appropriate Session # < 1, 2, 3, 4 or 5>
Session #: 1

UNKNOWN          Mon 07/29/2019   15:33:02
Password: *****

UNINITIALIZED
Automatic Equipment Identification System
APU Software Version: 5.1.1.130
Processing Version : Proc0330
CPU Type: LX800
Reader #0 Not Available at Startup
Reader #1 is not in current configuration
Running in Modemless Configuration
Mon 07/29/2019   15:33:05
Host Reporting: Off
Last LOGON: Mon 07/29/19   15:21:32

USID:          00000000
Site Name:     UNKNOWN
APU102XP:Main 1>

```

Figure 3

The username is “aei”; the default password is “secret”.

Once entered, the familiar session menu is displayed. Operation at this point duplicates earlier software versions. Select a session and login as usual.

See discussion of the passwd command for instructions to change the SSH passwords.

SSH Passwords

IMPORTANT: The passwords used to establish an SSH connection are not the same as the passwords used by the AEI application.

File Transfers

File transfers between the APU102 and a user may be performed using SCP protocol (which operates over SSH).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 7/15

A separate username and password are used to perform file transfers. The credential may vary based on your board configuration:

- LX800
 - Username: **update**
 - Default password: **secret**
- T10
 - Username: **aeiSCP** or **aeiTransfer**
 - Default password: **secret**

SCP also operates over port 22. If the APU can accept SSH connections, SCP will work.

There are various SCP clients available; the example demonstrates WinSCP which is a free program available for download on the internet.

Disclaimer

Comet Electronics makes no guarantees whatsoever regarding the suitability or security of any third-party software such as WinSCP, PuTTY, or TeraTerm.

It is up to the user to establish that software is genuine, properly licensed, and compliant with any company Information Technology (IT) policies.

When in doubt, contact your IT department for guidance.

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

WinSCP provides a graphical user interface (Figure 2):

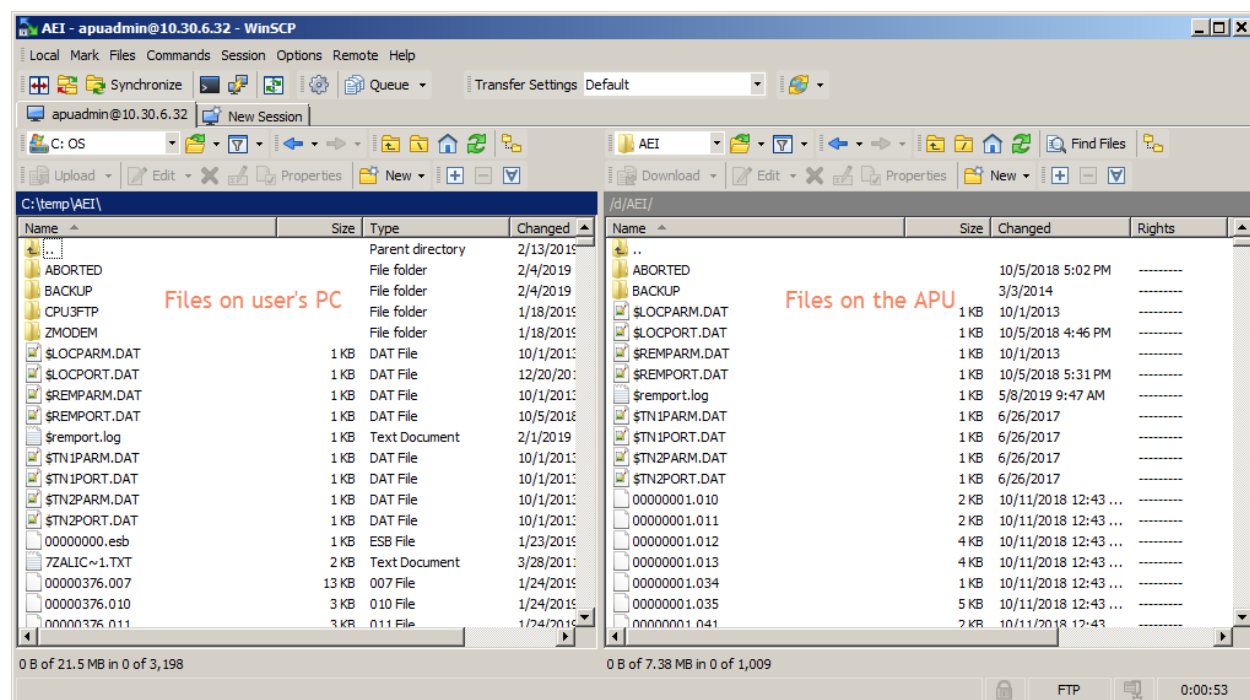


Figure 2

Before sending files to the APU102, make sure that the correct directory (/d/AEI) is selected.

Caution

Caution must be used when transferring files: changing or deleting files on the APU can render it inoperable.

Likewise, changing or deleting files on the user's PC can render it inoperable.

Updating your SSH password

Ensure that you update your SSH password. This workflow may vary depending on whether you are using LX800 or T10 board configurations.

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 9/15

Caution

While Comet Electronics LLC provides a temporary password, it is the customer's responsibility to establish new, secure passwords. Even on secure servers, data can be vulnerable if passwords are weak. Choose strong, unique passwords to protect your information.

Blank passwords are not allowed. Passwords must be between 6 and 30 characters long and are case-sensitive.

NOTE: SSH passwords are not stored on the APU102; a cryptographic hash² is stored. For this reason, recovery of a current password may not be possible.

Although the length of a password cannot be determined from the hash, users should be aware that common (weak) passwords like "password", "passw0rd", "secret", etc. are not secure because lists of thousands of hashed passwords are available with software that can match a stored hash to its clear-text entry in a list.

LX800

The PASSWD command, available only in the Session 1 Change mode, is used to set SSH passwords.

```
passwd aei|update [new_password] [new_password_again]
```

The passwd command requires a username, either aei or update, and the new password twice (to reduce the changes of accidentally entering a password with a typo making it difficult to connect later).

If the new passwords are not supplied, the user will be prompted to enter them.

```
APU102XP:Change 1>passwd aei MyNewPassword
Re-enter new password: *****
Password changed.
```

² A cryptographic hash is a value calculated from data for which there is no practical means to "un-hash" the hash value to reveal the original data. For passwords, it is important to note that it is possible to compare a hash to values in a database containing possible passwords and their hashed value. Database files containing many thousands of password/hash pairs are widely available.

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 10/15

```
APU102XP:Change 1>passwd update
Enter new password: *****
Re-enter new password: *****
Password changed.
```

T110

The SSHPASSWORD command, available only in the Session 1 change mod, is used to change the password of SSH accounts.

After typing the sshpasswd command, the user is prompted to give the name of the account they'd like to change the password for. This can be aei, aeiSCP, or aeiTransfer. After entering the chosen account name, the user is asked to input the password they'd like to use for the account, then confirm it.

```
APU102XPChange 1>sshpaswd
```

```
Username to change password of: aeiSCP | aeiTransfer | aei
```

```
Password: myNewPassword
```

```
Confirm Password: myNewPassword
```

```
The user [user_here]'s password was successfully updated
```

Password Recovery Procedure

If you cannot connect to the APU102 due to lost passwords, complete the recovery procedure below to reset SSH passwords to their default value.

1. Turn off power to the APU102.
2. Press and hold the SYS button while restoring power; keep pressing the SYS button.
3. After a minute or two, the SYS LED will blink five times – keep holding the button until the LED begins to blink again (at a faster rate than before).
4. Release the button; the unit will start with the default passwords set.

NOTE: The recovery procedure requires physical access to the APU102.

NETMRS

If the AEI application software fails to run, the unit will fallback to NETMRS which provides console access to allow remote troubleshooting.

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 11/15

Telnet serves as a backup means of communications when NETMRS is running: NETMRS allows Telnet connections even if SSH is enabled (SSH is available as well). If SSH is enabled, SCP will also be available.

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 12/15

Appendix A - Open Source Licenses and Acknowledgements

dropbear – SSH server

<https://matt.ucc.asn.au/dropbear/dropbear.html>

<https://github.com/mkj/dropbear>

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 13/15

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved.

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt. strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 14/15

THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

Copyright 2008, Google Inc.
All rights reserved.

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

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

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.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

curve25519-donna: Curve25519 elliptic curve, public key function

<http://code.google.com/p/curve25519-donna/>

Adam Langley <agl@imperialviolet.org>

Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).

SSH Installation Procedure		
Revision: 3	Revision Date: 7/16/2025 3:46 PM.	
Doc #: 480017		Page 15/15

More information about curve25519 can be found here

<http://cryp.to/ecdh.html>

djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

This is, almost, a clean room reimplementation from the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

Comet Electronics Proprietary Information

This document is the property of Comet Electronics, LLC. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the written consent of Comet Electronics. In addition, this document could contain technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (title 22, U.S.C. Sec 2751, et seq.) Or the Export Administration Act of 1979, as amended (title 50, U.S.C., app. 2401, et seq.).