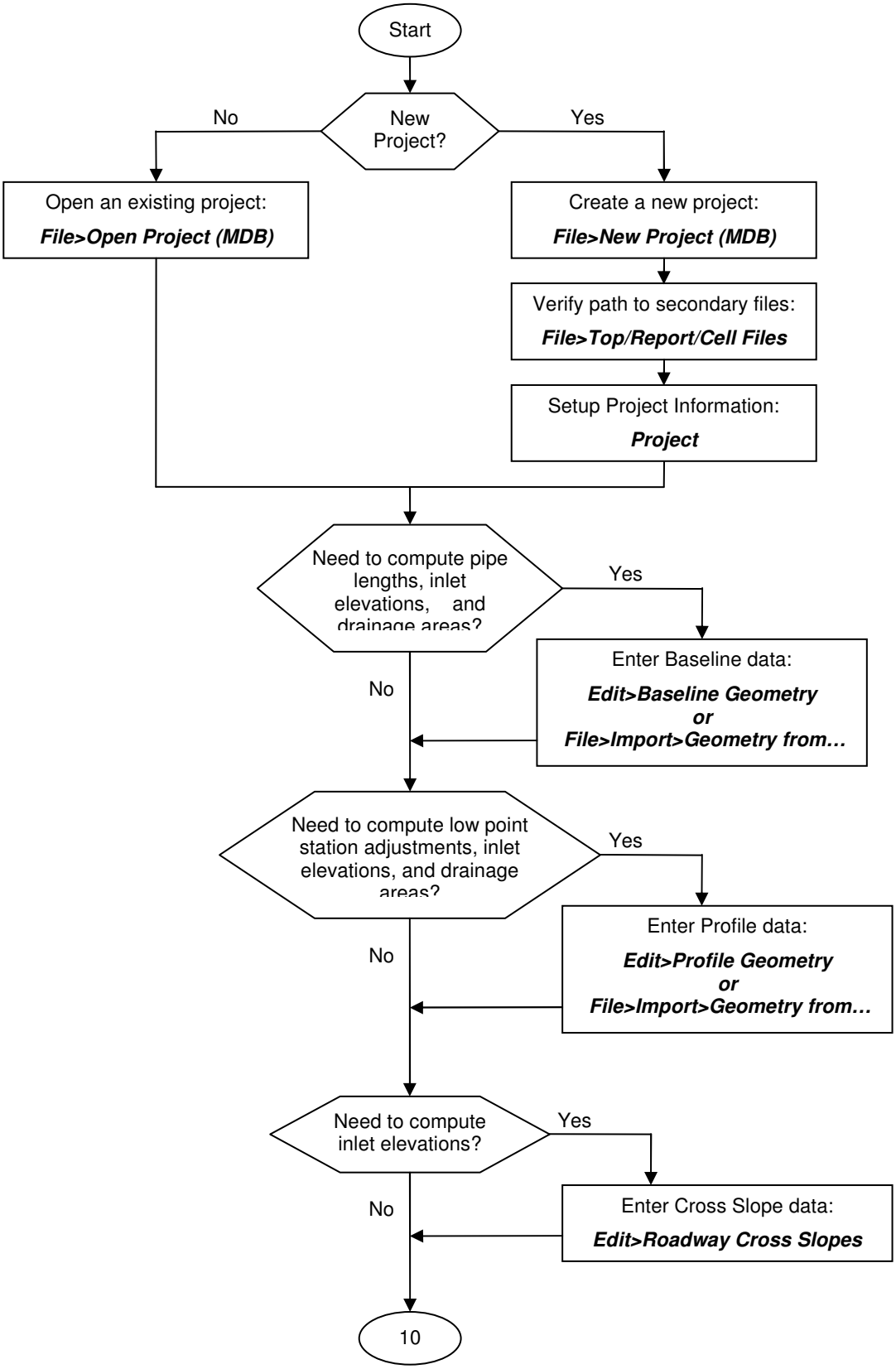
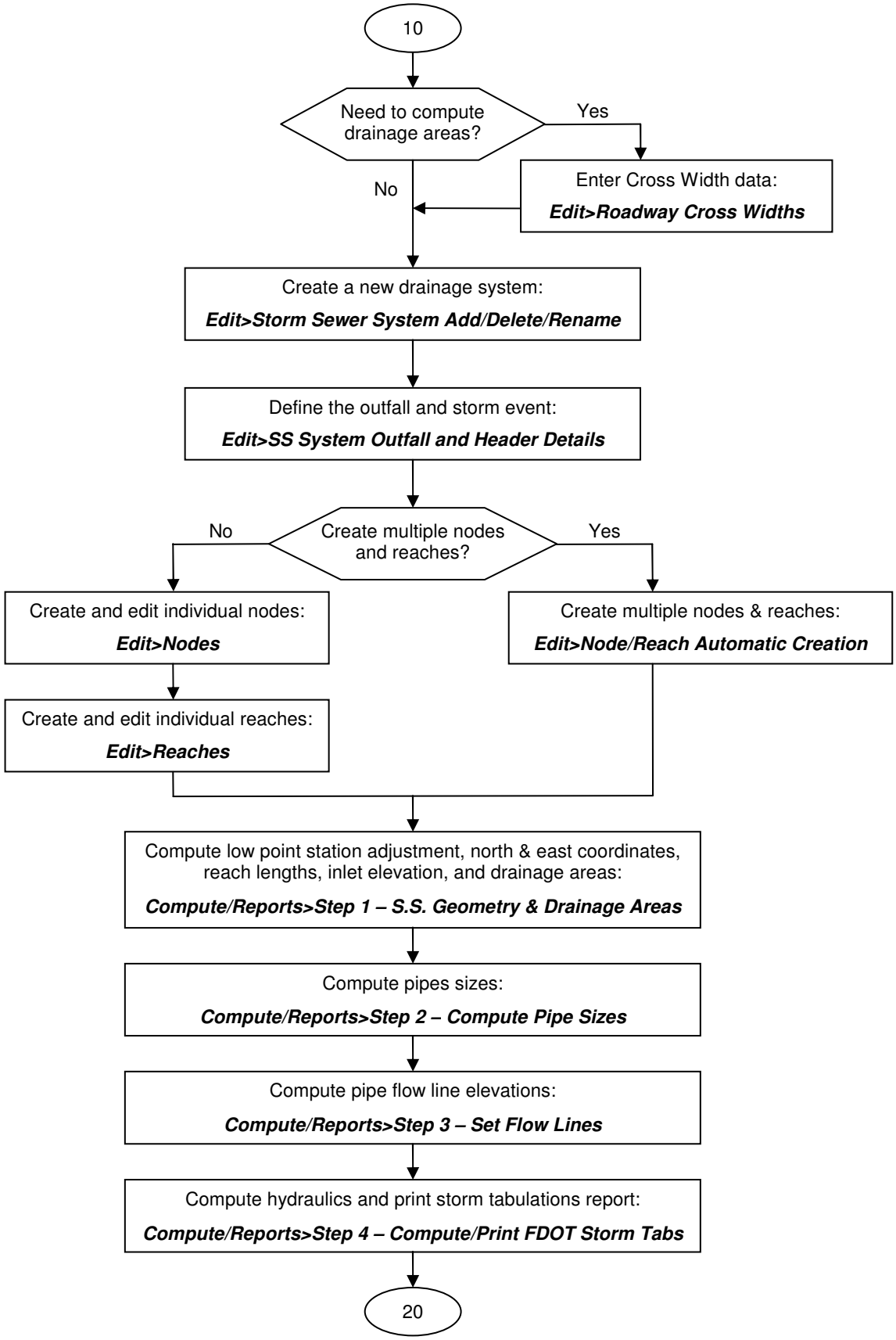
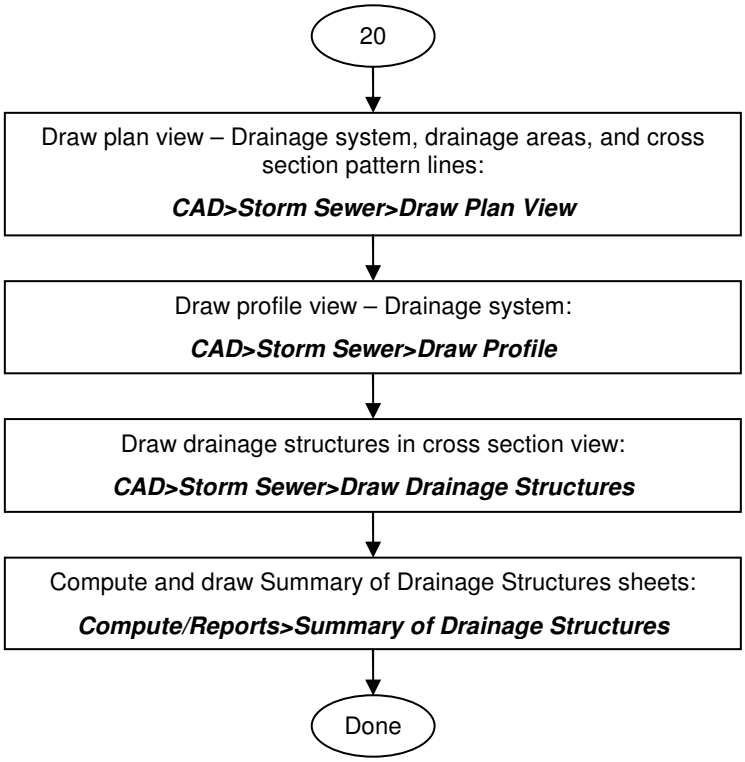
Appendix A: Step-By-Step User Flowchart




10
Need to compute drainage areas?
Yes
No
Enter Cross Width data:
Edit>Roadway Cross Widths
Create a new drainage system:
Edit>Storm Sewer System Add/Delete/Rename
Define the outfall and storm event:
Edit>SS System Outfall and Header Details
Create multiple nodes and reaches?
No
Yes
Create and edit individual nodes:
Edit>Nodes
Create multiple nodes & reaches:
Edit>Node/Reach Automatic Creation
Create and edit individual reaches:
Edit>Reaches
Compute low point station adjustment, north & east coordinates, reach lengths, inlet elevation, and drainage areas:
Compute/Reports>Step 1 – S.S. Geometry & Drainage Areas
Compute pipes sizes:
Compute/Reports>Step 2 – Compute Pipe Sizes
Compute pipe flow line elevations:
Compute/Reports>Step 3 – Set Flow Lines
Compute hydraulics and print storm tabulations report:
Compute/Reports>Step 4 – Compute/Print FDOT Storm Tabs
20


20
Draw plan view – Drainage system, drainage areas, and cross section pattern lines:
CAD>Storm Sewer>Draw Plan View
Draw profile view – Drainage system:
CAD>Storm Sewer>Draw Profile
Draw drainage structures in cross section view:
CAD>Storm Sewer>Draw Drainage Structures
Compute and draw Summary of Drainage Structures sheets:
Compute/Reports>Summary of Drainage Structures
Done

Appendix B: The History and Future of ASAD Locking Mechanisms

Weekly Code: From the beginning there has always been the Weekly code that will bypass all other forms of security. This is a code that changes every Monday morning at midnight. To get the weekly code call tech support at (352) 383-4191. We typically give out this code (and sometimes many weeks worth of codes) for the following reasons:

- A new user is evaluating ASAD for purchase.
- A HardLock Key has failed or is misplaced.
- A user is having a problem with one of the other locking mechanisms. We will not let a lock/driver problem keep a user from using ASAD. We will always give the user the weekly code first (to get you up and running) and solve the problem second.
- A user wants to take ASAD out of the office but doesn't want to take a lock.
- A user temporarily (for a month or so) needs access to more ASAD seats than their license(s) provide. This typically occurs during project submittal periods. This is meant to be a stop-gap measure to help users get past a busy period with few hassles. During a submittal, the last thing a user wants is to wrangle with their accounting department or the home office about the purchase of another license. Even though we are glad to offer this service, which is a service you won't find from other software companies, we do reserve the right to deny a user the weekly code if we feel the user is taking advantage of us.

The weekly code has been very successful and we will continue use it as one of our locking mechanisms.

HardLock Key: From 1996 to 2005, our frontline of software security has been the HardLock LT Key provided by Aladdin Knowledge Systems. In 2005, Aladdin discontinued the Hardlock LT and their support for the LT drivers. Around this time we started having conflicts between our older lock drivers and newer locks and drivers used by ICPR (by Streamline Technologies). ICPR had made the switch to Aladdin's newer locks (along with newer drivers). This conflict in lock drivers prevents ASAD from starting when the ICPR lock driver is installed and vice versa. The only immediate solution was to have the user un-install the lock drivers for one software, and re-install lock drivers for the other. Well, making a user un-install and re-install the lock driver a couple of times a day is not something we can live with. We had to have a solution quickly. However, buying, keying and distributing a couple hundred locks is not a quick task. Knowing that we would be using new locking mechanisms in the future, we decided to take the time to explore other locking options, including network licensing (LAN) and wide-area network (WAN). During this period, 05'-06', we turned to a little known routine we use during in-house programming and testing…the Registration file.

Registration File: The Registration File is a simple two line text file that we provide to the user. For new licenses, purchased in 05' or 06', the Registration File takes the place of the HardLock Key. In other cases where the HardLock Key fails, is lost or stolen, or conflicts with other locks/drivers, we will issue a Registration File to take the place of the HardLock Key. We usually include this file on the installation disk. However, sometimes we will send it as an email attachment or talk the user through creating it themselves. In the latter case, the user only needs to use Notepad.exe to create/edit the file. The Registration File's path and name are:

C:\windows\system32\AADEPZ3.INI or

C:\winnt\system32\AADEPZ3.INI

This file contains two lines of text which have to 'match-up' exactly for ASAD to run. The first line of text is the Company or Organization name. The second line, the code line, is a string of numbers that is a function of the first line of text. Here is an example (by the way, these example codes do not work):

ABC Engineering Company, Inc.

41426-891822

Even the slightest change in the first line will require a larger change in the second line. Note, in the two lines below the first line has had the (.) period removed after the 'Inc'. This results in the code line changing significantly.

ABC Engineering Company, Inc

43428-5521

If you have any questions about ASAD locking mechanisms, please call tech support at (352) 383-4191.

Appendix C: Installing and Un-Installing the ASAD CAD Engine.

ASAD's CAD Engine is Provided by Pangaea Cad Solutions (PCS), Ontario, Canada: Using PCS's 'PCSCustom' product, ASAD has the ability to read and write to MicroStation (V8 and V7) DGN files. The CAD engine module is PCSCUS.OCX and is located in the c:\windows\system32 (or equivalent) subdirectory.

CAD Engine Versions Used by ASADv2 and ASADv3: ASAD version 2 is only compatible with MicroStation V7 files. It uses an older version of the CAD engine, PCSCUS.OCX version 5.3.40.9. ASAD version 3, which uses a newer version of the CAD engine, is currently setup to run the CAD engine in the V8 mode only and therefore is compatible with MicroStation V8 files only. ASAD version 3 will eventually be setup to run the CAD engine in both V7 and V8 modes. ASAD version 3 uses PCSCUS.OCX version 6.6.10.24 or later. Both of these PCSCUS.OCX versions can be found on the installation CD:

d:\Install_files\CAD Engine files\ASADv2\Pcscus_5.4.40.9.ocx
d:\Install_files\CAD Engine files\ASADv3\Pcscus_6.7.12.19.ocx (or later)

Problem Running ASADv2 and ASADv3 on the Same Computer: As a rule, both versions of ASAD cannot be installed on the same computer at the same time. They will install into different directories and the ASAD programs (ASAD.EXE and ASAD3.EXE) will not conflict with each other, however the installation process will write its own version of PCSCUS.OCX into the c:\windows\system32 subdirectory. Therefore, only the last version of ASAD installed will run properly.

Getting ASADv2 and ASADv3 to Run on the Same Computer: The above section illustrated the rule…here's the exception to that rule. Un-register (in the windows system registry) the CAD engine, replace the CAD engine file, and re-register the CAD engine. Stop here and get your IT guy!! Most IT managers will be not be comfortable with novice users messing around with the system registry and will typically not allow users access to the \windows\system32 subdirectory or the **regsvr32** program. Now that you have the okay (or assistance from) the IT department, follow these steps:

Step 1: Un-Register the Current CAD engine.

From the desktop, click on Start>Programs>Accessories>Command Prompt (see figure C.1) to open the 'Command Prompt' window (see figure C.2). Change to the c:\windows\system32 (or equivalent) subdirectory by keying ***CD\windows\system32***and press enter.

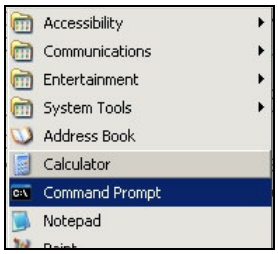


Figure C.1

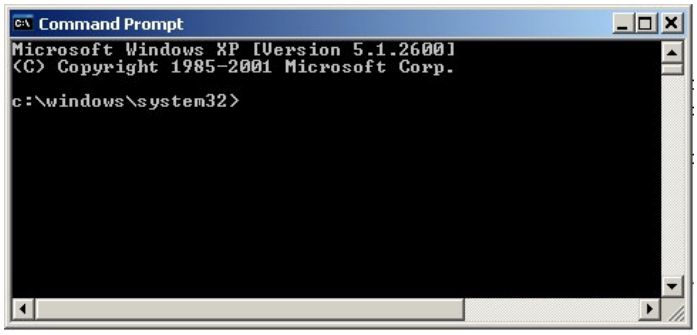


Figure C.2

At the 'c:\windows\system32>' prompt, key in ***regsvr32 /u pcscus.ocx*** and press enter (see figure C.3). When the file is unregistered a message box will notify the user (see figure C.4).

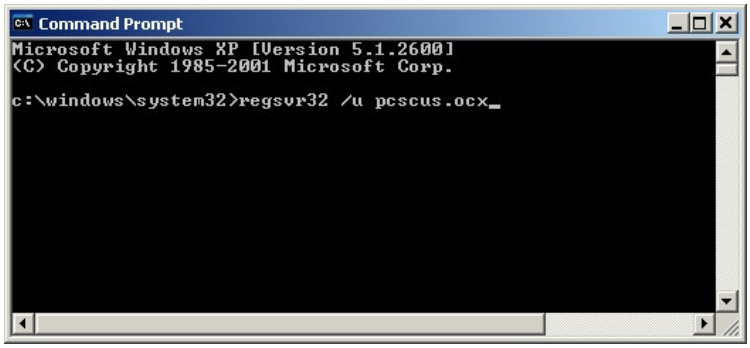


Figure C.3

Figure C.4

Step 2: Copy the New CAD Engine

If you want to run ASADv2 then use Windows Explorer to:

Copy **d:\Install_files\CAD Engine files\ASADv2\Pcscus_5.4.40.9.ocx**
To **c:\windows\system32\pcscus.ocx**

If you want to run ASADv3 then use Windows Explorer to:

Copy **d:\Install_files\CAD Engine files\ASADv3\Pcscus_6.6.12.20.ocx** (or later)
To **c:\windows\system32\pcscus.ocx**

Step 3: Register the New CAD engine.

Following the same procedure as Step 1, open the Command Prompt window and change to the c:\windows\system32 (or equivalent) subdirectory. At the 'c:\windows\system32>' prompt, keyin ***regsvr32 pcscus.ocx*** and press enter (see figure C.5). When the file is registered a message box will notify the user (see figure C.6)

Figure C.5

Figure C.6

Step 4: The Register Process Complete. Now start ASAD or ASAD3

Appendix D: Installing the Hardware Lock

WARNING: ***DO NOT insert your ASAD lock until after the software has been installed!***

The following installation procedures are for two different types of ASAD locks.

1. The Network lock allows user(s) to access the ASAD lock across a local area network. Typically the lock is located on a 'server' computer while ASAD is run on a 'client' computer.
2. The Standalone lock is located directly on the computer running ASAD.

These two locks are different and not interchangeable in their usage. To obtain a different type of lock, contact HES, Inc. at (352) 383-4191 or sales@hiteshew.com

The hardware lock installation process can be run from the ASAD installation CD or ***(after ASAD is installed)*** the ASADv3 subdirectory. The following documentation illustrates the procedure as run from the ASADv3 subdirectory (typically C:\Program Files\ASADv3)

NETWORK Lock

This section addresses the following items:

- Setting up the Server
- Setting up the Clients
- Test and troubleshoot the client/server communications.

1) Set up the lock SERVER.

NOTE: If ASAD is not installed on the server computer, then the following process may be run from the ASAD installation CD. Use subdirectory: 'D:\Lock Setup\Network\Server…' instead of 'C:\Program Files\ASADv3\Lock Setup\Network\Server...'

a) Run the 'Install.exe' program from the 'C:\Program Files\ASADv3\Lock Setup\Network\Server...' subdirectory. (see figure C.7)

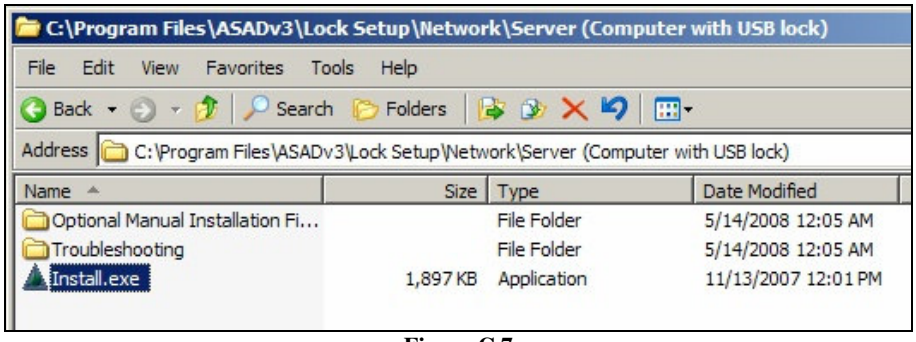


Figure C.7

b) Select 'USB' Dongle and the 'Server' radio button. Click 'Begin Install'. (see figure C.8)

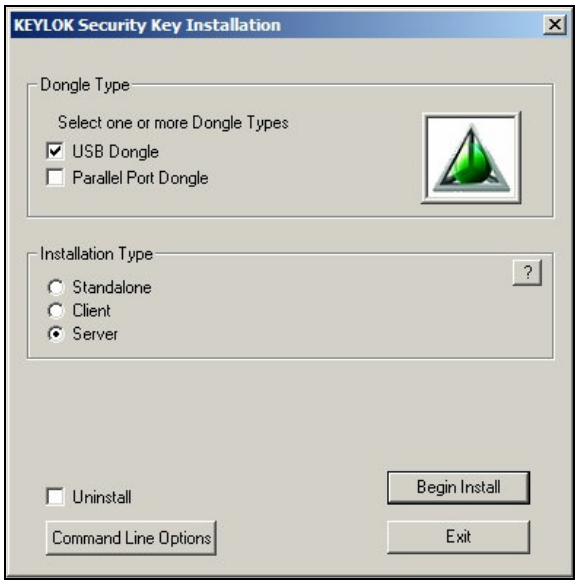


Figure C.8

c) Now insert your ASAD lock into the USB port. Windows will automatically detect the new hardware.

d) Using Task Manager, verify that the 'klserver.exe' process is running. (see figure C.9)

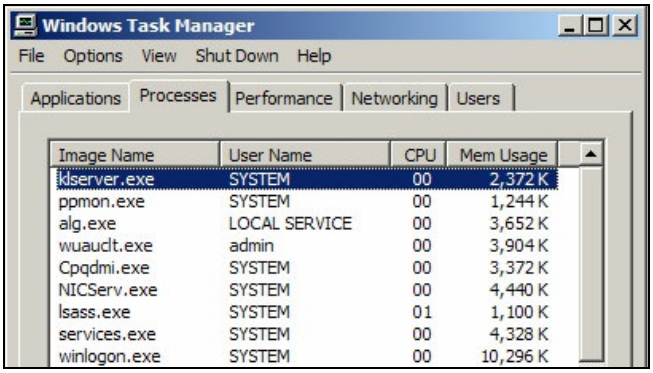


Figure C.9

2) Set up each ASAD user's computer as a CLIENT.

a) Run the 'Install.exe' program from the 'C:\Program Files\ASADv3\Lock Setup\Network\Client..' subdirectory. (see figure C.10)

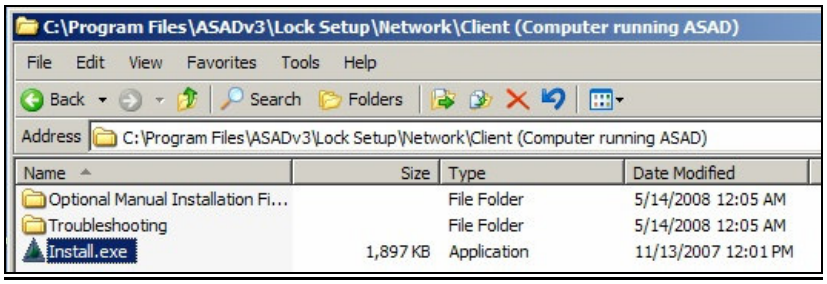


Figure C.10

b) Select the 'Client' radio button. Click 'Begin Install' (see figure C.11)

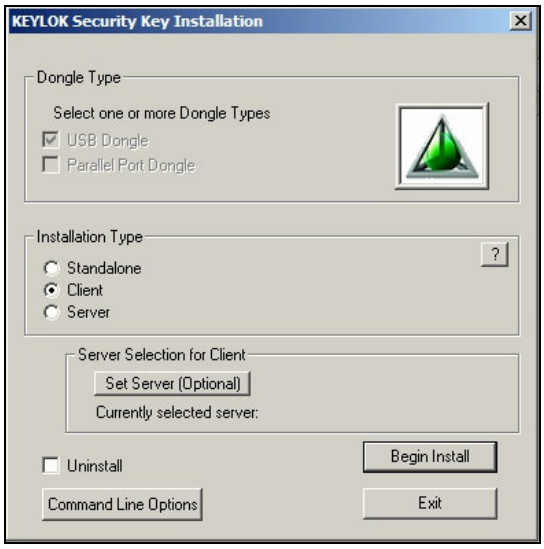


Figure C.11

3) Test and troubleshoot the client/server communications using the following procedures:

- Device Access Over a Network (Overview)
- Run VerifyNetworkKey.exe program.
- Run NetKeyMonitor.exe program.
- Stop/Restart KLSERVER.EXE process.
- Allowing a path through your Firewall

a) Device Access Over a Network (Overview)

General Information

The ASAD security system can be used to share a single lock among multiple copies of the ASAD application running on a network. The advantage of this technique is that multiple nodes can be controlled through use of a single lock. A server application is provided that communicates with the ASAD lock installed on the machine on which the server application is running. This technique should work on any network operating system running the TCP/IP protocol, which is currently the most widely supported network protocol. A protected program (ASAD) running on any node on the network can then access the lock via the network, up to the established maximum simultaneous user count. See figure C.12

Networking Components

The following components are required to implement the ASAD network security system. Each of these components is installed and configured automatically as appropriate by the lock install utility.

Server Application: This is the program that each copy of ASAD communicates with in order to acquire contact with the security device. This program acts as the interface between ASAD and the device driver, which actually communicates with the lock. The name of the server application is *KLSERVER.EXE*. The server runs as a Windows service. Any number of copies of this server can be run on any network.

NOTE: The server application (KLSERVER.EXE) can be installed and run on any machine, it does not require a server OS.

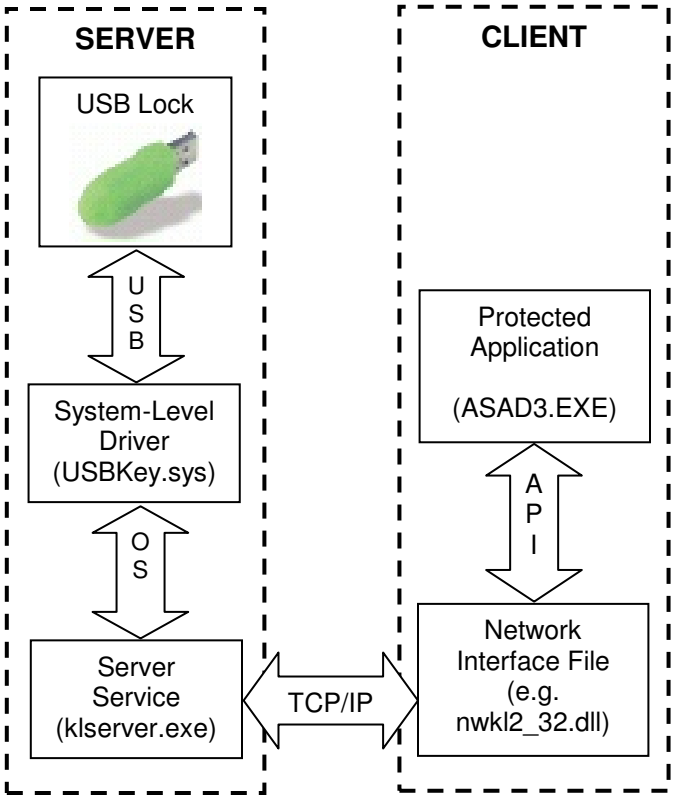


Figure C.12

Device Driver: This is the program that actually communicates directly with the lock. The server application communicates with this driver. The name of the device driver file for parallel port devices is *PARCLASS.SYS* for Windows NT/2000/XP/Vista and *PARCLASS.VXD* for Windows 95/98/ME. For USB devices, the device driver is *USBKey.sys* and it resides in the \Windows\System32\Drivers subdirectory.

ASAD lock: The lock required for network operation is identical to that used for standalone operation except that for more than one simultaneous user you must use special multi-user versions of the ASAD lock. The device must be physically installed on the network node that is running the server application *KLSERVER.EXE*.

Client Application (ASAD): **ASAD3.EXE** is the protected program that must be capable of communicating with the lock over the network in order to confirm the presence of the proper lock device, and to be able to read and/or write to the lock's memory. The protected application can also be run on the same computer platform as the server application. You can optionally force a client to attempt to attach to a specific lock server by including a file named *TCPIPSVR.DAT* that contains the IP address or network name of the desired dongle server. *TCPIPSVR.DAT* should be a standard ASCII text file and should be in the application directory or \Windows\System32.

Network: The computers on which the client application (ASAD) and server application is running must be physically connected via a network with the TCP/IP protocol supported on each platform. The server and all clients must be in the same subnet. Clients can be forced to use a specific server by a *TCPIPSVR.DAT* file in the \Windows\System32 directory on Windows NT/2000/XP systems (\Windows\System on Windows 9x/ME systems). The *TCPIPSVR.DAT* file is an ordinary text file that contains the network name or IP address of the server to which you want the client to connect. Note that a blank *TCPIPSVR.DAT* file is created by default during a Client installation; if a server name or IP address is specified during the installation, it will be written into the *TCPIPSVR.DAT* file.

Network Utilities: We provide two utilities to assist in implementing and monitoring networked dongles (locks). These utilities are as follows:

- NetKeyMonitor.exe is a utility that can be run on the dongle (lock) server or client platform. The utility shows all active servers detected on the network and reports the maximum number of allowed sessions as programmed into the security device, as well as the current number of active sessions.
- VerifyNetworkKey.exe is a utility that allows you to make sure that a client on a network can communicate with a dongle (lock) mounted on a remote server. Its only function is to check for the presence of a network dongle (lock).

Both utilities can be found in the 'C:\Program Files\ASADv3\Lock Setup\Network' subdirectory.

ASAD lock specific search order is:

1) Search for local USB device
2) Search for local parallel device
3) Search for TCP/IP network key

b) Run VerifyNetworkKey.exe program (see figure C.13)

VerifyNetworkKey is a utility that allows you to make sure that a client on a network can communicate with a lock mounted on a remote server. Its only function is to check for the presence of a network dongle. Start this program the 'C:\Program Files\ASADv3\Lock Setup\Network' subdirectory .

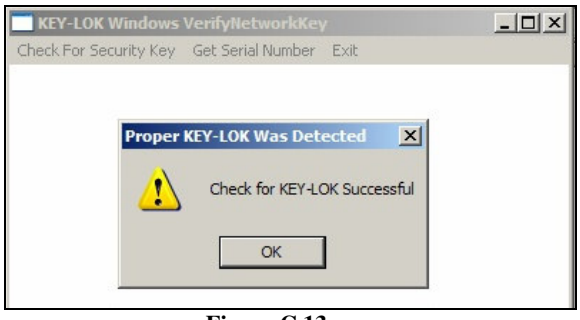


Figure C.13

c) Run NetKeyMonitor.exe program.

NetKeyMonitor is a utility that can be run on the dongle server or client platform. The utility shows all active servers detected on the network and reports the maximum number of allowed sessions as programmed into the lock device, as well as the current number of active sessions. Its only function is to check for the presence of network dongles, so you can safely send it to your end-users as a diagnostic tool. As seen in figure C.14, the network lock system is working properly.

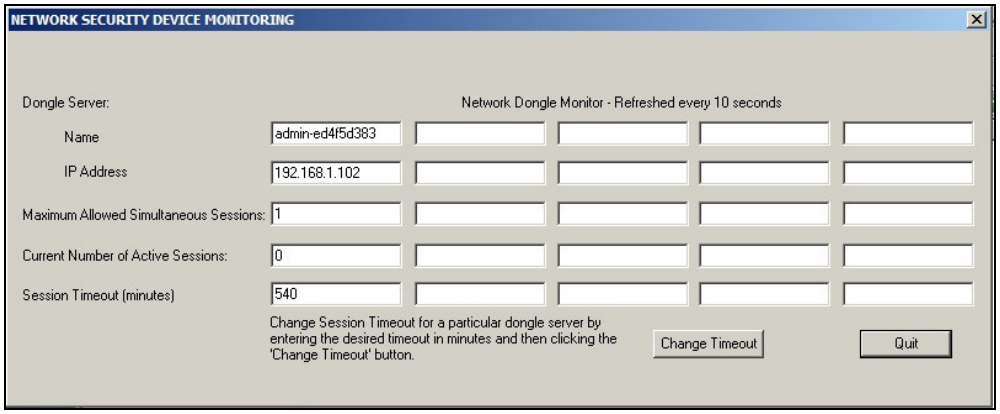


Figure C.14

Shown in figure C.15 is a network lock system NOT WORKING properly. Notice the 'No/Wrong Dongle' status in some fields. This problem is usually fixed by stopping and restarting the KLSERVER process (see below: 'Stop/Restart KLSERVER.EXE process') on the server.

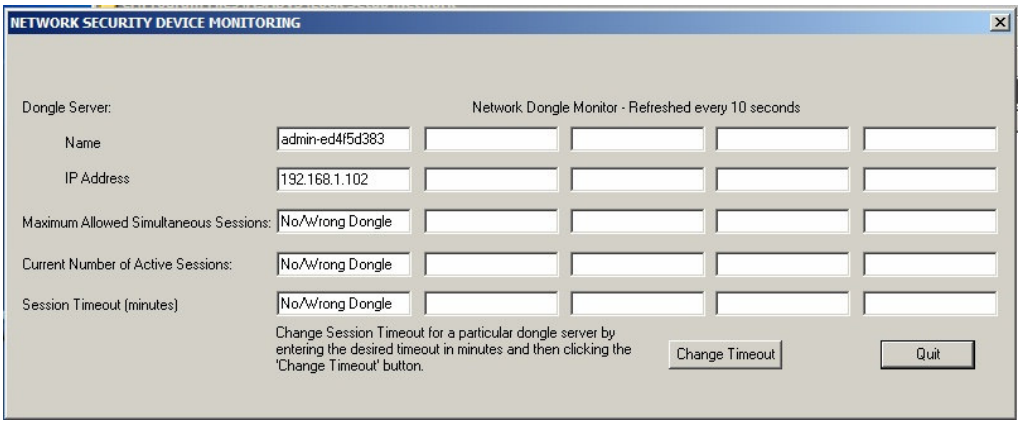


Figure C.15

d) Stop/Restart KLSERVER.EXE process.

After the server and clients have been setup and the lock is connected to the server, if ASAD fails to connect or the two previous utilities indicate a problem, then stopping and restarting the KLSERVER service may fix the problem:

Step 1: Stop KLSERVER. From the desktop, click on Start>Programs>Accessories>Command Prompt to open the 'Command Prompt' window. Key in ***net stop klserver*** and press enter. (see figure C.16)

Figure C.16

Step 2: Start KLSERVER. Key in ***net start klserver*** and press enter. (see figure C.17)

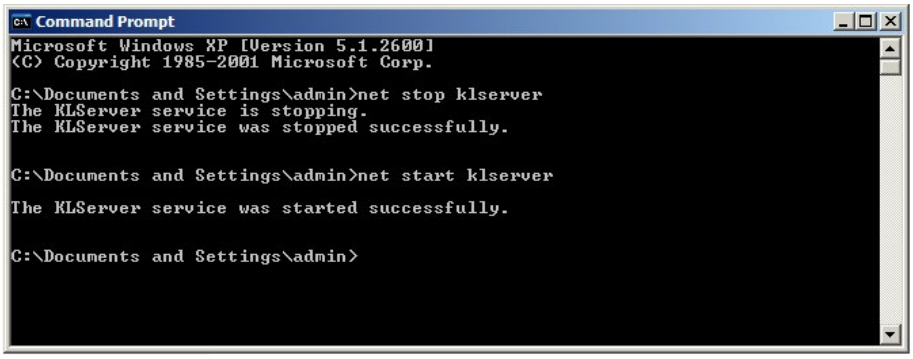


Figure C.17

e) Allowing a path through your Firewall.
In order for a client application (ASAD) to communicate with a lock server via TCP/IP, verify that no firewalls or security software on client or server or routers settings are blocking communications. All firewalls, security software, and routers must be set up to allow **klserver.exe** and **ASAD3.exe** to communicate via TCP/IP, and must allow communications via TCP/IP port 4242. In addition, if you are not using a TCPIPSVR.DAT file to point the client to a specific server, all firewalls, security software, and routers must be set up to allow UDP communications between client and server.

STANDALONE Lock

This section addresses the following items:

- Install lock drivers and lock
- Test the Lock

1) Install lock drivers and lock

a) Run the 'Install.exe' program from the 'C:\Program Files\ASADv3\Lock Setup\Network\Server...' subdirectory. (see figure C.18)

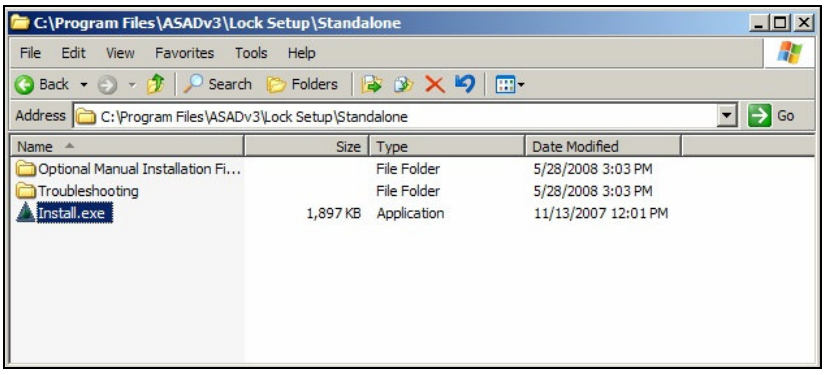


Figure C.18

b) Select 'USB Dongle' and the 'Standalone' radio button. Click 'Begin Install' (see figure C.19)

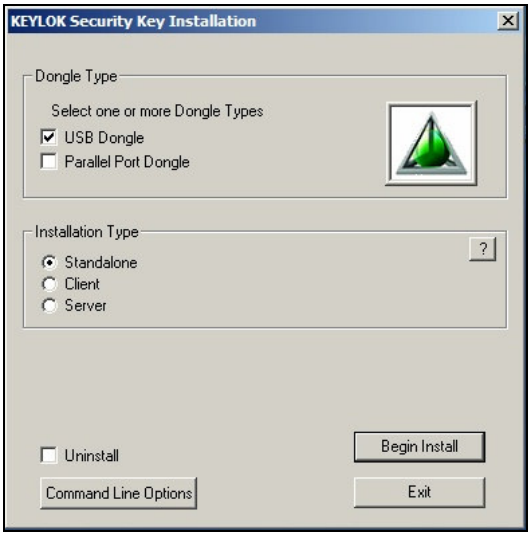


Figure C.19

Figure C.20

c) Now insert your ASAD lock into the USB port. Windows will automatically detect the new hardware.

2) Test the lock, run VerifyKey.exe program (see figure C.21).

VerifyKey.exe is a utility that allows you to make sure that the standalone lock is connected and the drivers are communicating properly. Start this program from the 'C:\Program Files\ASADv3\Lock Setup\Standalone\Troubleshooting' subdirectory.

Note: the Serial Number will be different for each lock.

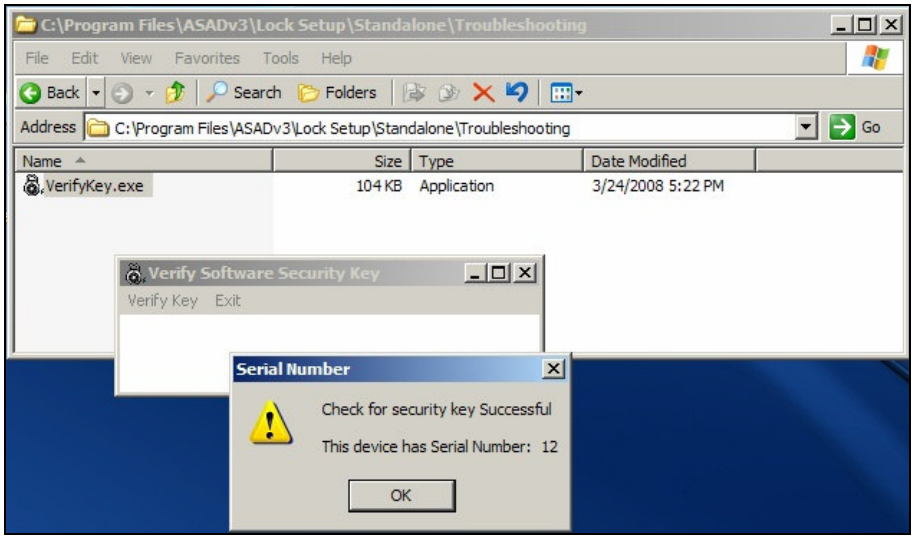


Figure C.21