SAND2014-0360P

EDAS User Manual

Jay Brotz and Maikael Thomas

Revision 0.1, 01/10/2014

Document Introduction

This document is meant to instruct users on the installation and use of the Enhanced Data Authentication System (EDAS). A brief introduction to the product, including a description of hardware and software, is followed by instructions for installing and using the system.

EDAS Introduction

The Enhanced Data Authentication System (EDAS) is a device to securely "branch" measurement data from operator-owned instrumentation to a Safeguards inspectorate, while guaranteeing the integrity of the operator communication link. While Safeguards normally depend on measurements that are fully independent from those of the operator, certain situations may call for the sharing of information from facility systems for both operations and verification purposes. An inspector must be confident that this branched information is a secure, true, and complete replica of the operator instrumentation. At the same time, an operator must have the assurance that the branching does not introduce an unacceptable risk to facility operations. The EDAS has been architected to meet the requirements of both parties.

EDAS operates as a server that lies in between operator equipment and an operator computer. All data that is transferred between the operator systems are recorded without affecting the operator communications, and the recorded data is sent to an inspector computer where it is processed by the EDAS Client software. The EDAS Client software saves each data packet, along with pertinent information about that packet, to a text file that can then be interfaced to other data systems (such as the RADAR system).

EDAS Server Hardware Description

The EDAS Server is composed of a Beagle Bone Black embedded ARM processor board with a custom cape (stacking accessory board) that connects two serial connections and records all data being transferred over those connections with an isolated sensing mechanism. The serial connections are made with DB-9 connectors (one male and one female) that are using either RS232 or RS485 protocol. Communication from the EDAS Server to the inspector computer can be done by Ethernet with the RJ-45 jack or Ethernet over USB with the mini USB jack. **Please note that we recommend connecting the inspector computer to the EDAS using the USB connection as it will provide networking and power for the EDAS in one standardized connection.**

EDAS Server Firmware Description

The EDAS Server firmware collects all data transferred over the serial connections, compiles them into discrete packets, signs them using an elliptic curve digital signature algorithm (ECDSA), encrypts the packets (note that this is currently disabled), and sends them over a socket connection to the EDAS Client software running on the inspector computer. In addition, the EDAS Server creates heartbeat messages at a configurable frequency that are also sent to the inspector computer.

EDAS Client Software Description

The EDAS Client software opens a socket connection with the EDAS Server and receives data packets as they are created. It then saves the data packets to a comma-separated values (CSV) file with the format shown in Table 1. Note that each field in the table is separated by a comma in the file and each entry (message) is separated by a new line.

Table 1. EDAS Client Output File Format

Field	Description
Received Date/Time	ASCII text representation of the date and time that the EDAS Client received a message, in the format YYYY-MM-DD hh:mm:ss, where YYYY is the four-digit year, MM is the two-digit month, DD is the two-digit day, hh is the two-digit hour, mm is the two-digit minute, and ss is the two-digit second
Message Type	Either ‘DATA’ for data messages,’ HEARTBEAT’ for heartbeat messages,

	'ENCRYPTION_FAILURE' for any message that could not be decrypted by the EDAS Client, or 'PUBLIC_KEY_QX' or 'PUBLIC_KEY_QY' to transmit the ECDSA public keys from server to client.
Message ID	A number indicating order of message creation
EDAS Date/Time	The date and time that the EDAS Server created the message, in the same format as Received Date/Time
Data Source	Either 'operator equipment' or 'operator computer' for data messages (and none for heartbeat messages)
Data Size	The number of bytes in the data field
Data	ASCII text representation of the data read from the serial connection
Authentication Status	'Passed; or a reason for failure
Encryption Status	'Success' for all data messages and heartbeat messages, 'Failure' for all encryption failure messages

Setting up the PC Connection to the EDAS Server

1. Since these instructions involve changing network adapter settings, you must have administrator rights to the Windows PC that you are using. Before beginning these steps, make sure that you are logged in as an administrator or can enter an administrator password when asked.
2. Connect the EDAS Server to a Windows PC using a USB cable with a mini-B connector on one end (plugged into the EDAS).
3. Open a Windows Explorer window and click on 'Computer'. The EDAS should show up as a mounted drive with the name 'BeagleBone Getting Started' and a drive letter followed by a colon. Double-click it to open the BeagleBone file system as a mounted drive.
4. Go to 'Drivers'>'Windows'. If your operating system is 64-bit[1], run 'BONE_D64.exe'. If your operating system is 32-bit, run 'BONE_DRV.exe'.
5. When the driver installer is finished, unplug the EDAS from your computer and plug it in again.
6. Open the network adapter settings by going to the Start menu and opening the Control Panel. Then click on Network and Sharing Center. On the left bar, click on 'Change adapter settings'. You should see one adapter, probably named 'Local Area Connection x' where 'x' is a number, with the description of 'Unidentified network' and 'Linux USB Ethernet/RNDIS Gadget…". Right-click on this adapter and select Properties. If a dialog asks you to allow this action, select 'Yes'. On the 'Local Area Connection x Properties' window, click on 'Internet Protocol Version 4 (TCP/IPv4)' and then click the Properties button. Click the radio button 'Use the following IP address:' and in the IP address field, type 192.168.7.1. In the Subnet mask field, type 255.255.255.0. You can leave the rest of the fields as they are.

[1] To tell whether your operating system is 64-bit or 32-bit, go to the Start menu and select Control Panel in the bar at the right, then go to System. On the System page in the System section, a line that starts with 'System type:' specifies whether the operating system is 64-bit or 32-bit.

Installing EDAS Server Firmware

1. You will need three files supplied by Sandia National Laboratories: EDAS.jar, edas_config, and runEDAS.sh and some 3rd party libraries. The 3rd party libraries will be provided in a subdirectory called 'libs'.
2. You will also need one file, the Bouncy Castle cryptographic library, that you will download yourself[2]: bcprov-jdk15on-xxx.jar (the latest release as of 12/13/2013 is 1.50, which has a filename of bcprov-jdk15on-150.jar).
3. Move EDAS.jar, edas_config, and runEDAS.sh to the EDAS into /home/ubuntu using SCP or FTP[3]. Put all 3rd party libraries in a subdirectory called 'libs'.
4. Open an SSH session with the EDAS server using, for example, Putty[4]. The EDAS IP address is 192.168.7.2, the username is 'ubuntu' and the password is 'Euratom' (no quotes on either).
5. At the prompt below, type:

```
ubuntu@arm:~$ chmod +x runEDAS.sh
```

Installing EDAS Client Software

These instructions assume that the user is running Windows 7 on the computer that will host the EDAS Client software. While the software may also run on Windows XP, it has not been tested on that operating system. The software may also run on Mac OS X and modern Linux/Unix operating systems, but these instructions do not explain installation or use on these platforms.

1. You will need several files supplied by Sandia National Laboratories: EDASClient.jar, client_config, runEDASClient.cmd, and some 3rd party libraries. The 3rd party libraries will be provided in a subdirectory called 'libs'.
2. You will also need one file, the Bouncy Castle cryptographic library, that you will download yourself[5]: bcprov-jdk15on-xxx.jar (the latest release as of 12/13/2013 is 1.50, which has a filename of bcprov-jdk15on-150.jar).
3. Put EDASClient.jar, client_config, and runEDASClient.cmd in the desired run directory (such as C:\EDAS). Put all 3rd party libraries in a subdirectory called 'libs'.

EDAS Server Operation

1. Unplug the EDAS Server's USB connection and reconnect it to the computer that will have the EDAS Client software installed on it.
2. Connect a serial cable with a female DB-9 plug from the operator equipment (i.e., barcode scanner) to the male DB-9 receptacle on the EDAS Server.

---

[2] Go to http://www.bouncycastle.org/latest_release.html.
[3] If you do not have an SCP or FTP client, you can download PSCP and PSFTP from http:// http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.
[4] You can download Putty from http:// http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.
[5] Go to http://www.bouncycastle.org/latest_release.html.

3. Connect a serial cable with a male DB-9 plug from the operator computer to the female DB-9 receptacle on the EDAS Server.
4. Start the EDAS Server software by typing '/home/Ubuntu/startEDAS.sh'.
5. When the EDAS Client is running on the computer connected by USB to the EDAS Server, every data transmission going over the serial connection (in either direction) will be collected by EDAS and turned into a data packet that gets sent over the socket connection to the EDAS Client, if it is connected to a computer running the Client application. Also, EDAS will send a heartbeat at a configurable rate to the EDAS Client.
6. All log files are saved in the 'logs' subdirectory. The log file from today will be named 'edas.log'. All previous log files will be appended with a date stamp.

EDAS Server Configuration

The EDAS Server firmware can be configured by editing the edas_config file. The contents of the file are below:

```
*****************************
***         Server          ***
*****************************
<server_port>
54321
</server_port>
<server_stack>
1024
</server_stack>


*****************************
***      Packet Builder     ***
*****************************
<packet_builder>
0
Falses

200
FROM_READ
</packet_builder>
<source_file>
/dev/ttyO2
/dev/tty04
</source_file>
<verbose>
true
</verbose>
<heartbeat>
```

```
60
</heartbeat>
```

Each field in the configuration file begins with an open tag of the name of the field (i.e., <heartbeat>) and a close tag with the name of the field (i.e., </heartbeat>). The text between the open tag and the close tag sets the value of that field. Note that the value of the field must be on a separate line from both the open tag and the close untag. The fields are described in Table 2 below:

Table 2. EDAS configuration field

Field	Description
server_port	The TCP port that the EDAS Client must use to connect to the EDAS Server (the IP Address is always 192.168.7.2)
server_stack	The size of the data stack that the server can hold (in bytes)
packet_builder	Four fields in this order all separated by a new line: the size limit of a data packet (unlimited if 0), whether the size limit is a hard or soft limit[6] (true is a hard limit and false is a soft limit), the time limit of a single data packet in milliseconds, and the method of data packet creation[7].
source_file	The device mounted on the operating system that is to be read for serial data. This field must be '/dev/ttyO2' followed by '/dev/ttyO4' on a new line.
Verbose	A value of 'true' will send more information to the console output. Since the standard way of running the EDAS Server is in the background at boot up (automatically), this should normally be set to 'false'.
Heartbeat	The period of the heartbeat messages, in seconds

EDAS Client Operation

1. Connect the EDAS Server to the computer running the EDAS Client by USB.
2. Navigate to the install directory and double-click on EDASClient.cmd. It will open a Windows command line interface and show the console output of the EDAS Client software.
3. You will see the last message created before the EDAS Client connected to the EDAS Server (probably a heartbeat message if no data is being transmitted over the serial connection) followed by any future heartbeat or data messages.
4. All log files are saved in the 'logs' subdirectory. The log file from today will be named 'edas.log'. All previous log files will be appended with a date stamp.

[6] A hard size limit to a data packet means that only the number of bytes specified in the size limit field will be included in the data packet, whereas a soft size limit means that data packet creation will stop when more bytes than the size limit are read in, but all of that data will be in the data packet.

[7] A value of HEART_BEAT means that a data packet will be created every interval of the time limit field, whether or not data has been read. A value of FROM_READ means that a data packet will only be created after data is read in. A value of HYBRID means that from EDAS startup until data is read, the firmware is in HEART_BEAT mode, and thenceforth it is in FROM_READ mode.

5. All messages are saved in the file named 'messagesYYYY-MM-DD.csv' in the 'logs' directory (which is in the same directory as EDASClient.cmd) where YYYY is the year, MM is the two-digit month, and DD is the two-digit day. The format for this file is shown in Table 1.

EDAS Client Configuration

The EDAS Client software can be configured by editing the client_config file. The contents of the file are below:

```
*****************************
***         Server          ***
*****************************
<server_port>
54321
</server_port>
<server_address>
192.168.7.2
</server_address>
<verbose>
true
</verbose>
```

Each field in the configuration file begins with an open tag of the name of the field (i.e., <server_port>) and a close tag with the name of the field (i.e., </server_port>). The text between the open tag and the close tag sets the value of that field. Note that the value of the field must be on a separate line from both the open tag and the close untag. The fields are described in Table 2 below:

Table 3. EDAS configuration field

Field	Description
server_port	The TCP port that the EDAS Client uses to connect to the EDAS Server
server_address	The IP address of the EDAS Server (default is 192.168.7.2)
verbose	A value of 'true' will send more information to the command line window output

EDAS Cryptographic Authentication

Cryptographic authentication is important to protect the integrity of data transmitted between the EDAS server and client. The EDAS Server signs all messages using k-283 Elliptical Curve Digital Signature Algorithm (ECDSA). The server generates a private/public key pair using a random source provided by the operating system. The private key is protected by the EDAS Server, but it will send the public keys to the EDAS client upon establishing a connection. Only the server will be able to sign packets using the private key, but the client will be able to authenticate messages using the public key.