



# Criminal History Record Information Response Decryption Instructions

Illinois State Police • Bureau of Identification • 260 North Chicago Street • Joliet, Illinois 60432

## PURPOSE

This document details system requirements, installation instructions, and decryption instructions for the software necessary to receive and decrypt e-mail attachments sent by the Illinois State Police (ISP), Bureau of Identification (BOI).

## WHY DIGITAL ENCRYPTION?

All criminal history responses sent from the BOI across the internet in the form of e-mail are federally mandated to be encrypted and users to be authenticated. In compliance with this mandate, ISP will send out e-mail attachments that have been encrypted to the industry standard protocol.

Encryption will guarantee the security of the information contained in the response should it be intercepted by unauthorized persons while in transit. Authentication will guarantee the person receiving the encrypted response is the person intended and authorized to decrypt it.

## CHECKLIST/BEFORE YOU START:

- This process will require the uninstallation and installation of programs. If you are not authorized to add or remove programs on the PC, you may need to contact your IT staff for assistance.
- Know what Operating System and version (32 bit or 64 bit) is on the PC used for decrypting responses. *It is very important to note the version (32 bit or 64 bit) as this determines which software package must be downloaded and installed.*
  - To determine the Operating System/version:**
    - Click on the Start Button
    - Click on Settings/Control Panel or Control Panel
    - Click on System or System and Security/System
    - The Operating System and Version are shown on the “General” tab (if there is no notation of 64 bit under System, it is a 32 bit system).
- All Microsoft Security Updates must be installed prior to installation of the Entrust Security Provider software.
- Temporarily disable virus protection software. This can interfere with the installation of Entrust Security Provider software.

## SYSTEM REQUIREMENTS

---

The following operating systems are compatible with Entrust software:

- Microsoft Windows XP SP3 - Professional/Home/Tablet 32-bit Microsoft Windows Vista™ SP2 - All 32-bit and 64-bit editions
- Microsoft Windows 7 SP1 - All 32-bit and 64-bit editions
- Microsoft Windows Server 2003 SP2 - All 32-bit and 64-bit editions
- Microsoft Windows Server 2003 R2 SP2 - All 32-bit and 64-bit editions
- Microsoft Windows Server 2008 SP2 - All 32-bit and 64-bit editions
- Microsoft Windows Server 2008 R2 SP1 - All 64-bit editions
- *For Apple/Macintosh Computers, the link is <https://truepass01.illinois.gov/downloads/ESP/MAC/>*

## ENTRUST ENROLLMENT

---

Users must go to [www.illinois.gov/pki/](http://www.illinois.gov/pki/) to enroll with the State of Illinois to be issued a Digital Certificate required for use with Entrust software. Select the “*Get a Digital ID*” button located on the left side of the web page. The enrollee must be a real person with a valid Illinois driver’s license. Selected information from the driver’s license will be asked for during enrollment. It must be entered exactly as printed on the driver’s license.

Users must read and agree to the subscriber agreement with the State of Illinois Central Management Services. Out-of-state users must click the “*Non-Illinois Resident Accept*” button instead of the “*Agree*” button on the Subscriber Agreement form.

When entering names into the name fields, do not put a period (.) after the middle initial. The web site will allow the entry of one, but it causes problems elsewhere, so avoid doing this. Users will be asked to create a profile name and password. **Please remember these!** Write them down and keep them in a safe place.

The ISP Criminal History Record Information system is not capable of sending e-mail responses to more than one person. Therefore, only one person from each agency needs to be enrolled.

## DOWNLOADING AND INSTALLING ENTRUST

---

**Enrollment must be completed prior to downloading the Entrust Security Provider software.** The Entrust Security Provider software is available online and can be accessed via link to the download site on the Electronic Conviction Inquiries page of the ISP web site at [www.isp.state.il.us/crimhistory/chri.cfm](http://www.isp.state.il.us/crimhistory/chri.cfm).

Instructions for the installation and use of the **Entrust Security Provider** program are located at the link provided above.

After completing the installation of the ESP software, you must contact ISP Customer

Support to request a change to your agency's response method type. Please see the topic, "Activating E-mail Responses" below for instructions for contacting Customer Support. Responses received using the new method of decryption will be identified with the following in the subject line: **Your Criminal History Response or Your Criminal History Response – File of your Inquiries.**

## ENTRUST OPERATION

After the install is complete, the following icon will appear in the bottom right system tray



near the clock on the PC. The presence of the red **X** in the icon indicates that the user is not logged in to their digital ID. When the user is logged in, but the session has timed out (i.e. no activity for more than 30 minutes) the user will be logged out.

Double clicking this icon, the following window should appear.



Enter the Name (User ID) and the password that was created when registering for a State of Illinois Digital ID. If you forget the password for your Profile Name, you can go to the following URL: [www.illinois.gov/pki](http://www.illinois.gov/pki), then select the link to "Forgot Password". Follow the instructions to recover your password. Please do not call the ISP as we will not be able to reset passwords on the CMS Certificate Authority server.



After successfully logging in, the icon in the system tray will change: This icon indicates that the user is logged in to their digital ID.

To log out, right click the icon and choose the option "Log Out", or double click on the system tray icon again to log out.

## CHANGING YOUR RESPONSE METHOD TO E-MAIL

Once you have enrolled for your Digital Certificate, installed the Entrust Security Provider software, and can successfully log on to Entrust, you must fax the Illinois State Police Customer Support Unit on agency letterhead, at (815) 740-4401.

- Provide the Agency ORI
- Provide the e-mail address
- Provide the name of the agency contact person

The change will be made within 24 – 48 business hours. You will not receive any responses in your e-mail until the changes have been completed in the Criminal History Record Information system. Please ensure that the following email address is in your

email address book to prevent your responses from going to a spam folder:  
[ISP\\_CHRI\\_Response@isp.state.il.us](mailto:ISP_CHRI_Response@isp.state.il.us).

## **HOW TO DECRYPT A FILE**

---

If you do not sign onto Entrust before you try to decrypt a file, you will be prompted to sign onto Entrust when you try to open the file.

If the user has an installed client for their email (such as Microsoft Outlook, Mozilla Thunderbird, Lotus Notes, etc.) and the ESP software is installed the user will double click on the attachment in their email to open the criminal history response. If the user is not logged into Entrust, the software will ask for their Name (user ID) and password.

- 1) To open a response from with an installed email client (such as Microsoft Outlook or Lotus Notes):
  - a. Double click the response file in the email program and open the response directly from email or save the file to a folder on their computer prior to decryption.
  - b. Save the response to a folder on the computer, then either double click the file or right click the file and select "Decrypt and Verify" to begin the decryption process.
  - c. The first time a response is opened using either method will prompt the user to log into Entrust if they are not already logged in.
- 2) To open a response using a web based email client:
  - a. The response **must** be saved to a folder on the computer prior to decrypting.
  - b. After the response is saved to the computer, it can be decrypted by double clicking the file or right clicking the file and selecting "Decrypt".
- 3) To decrypt multiple responses with one click:
  - a. Save the response file(s) to a folder on the computer.
  - b. Go to the folder containing the files and select all files you wish to decrypt.
  - c. Right Click the selected files
  - d. On the right click menu that appears, select "Decrypt and Verify"

The user also has the option of saving the encrypted file to a location on their PC. This can be done for all users, but will be mandatory for any user who used a web client for their email. Once the file is on the local file system the user simply needs to double click on the response or right click and select "Decrypt and Verify" to start the decrypt process. This process is the same as for installed client email users. Clicking on the response will open the response in the default browser if the user is logged into Entrust, otherwise it will ask for the Name (user ID) and password and then proceed to decrypt the response. To decrypt multiple response files, select the files, right click, and select "Decrypt and Verify".

When the file is opening the user will be prompted with the following message:

*"Opening an encrypted or digitally signed file will launch the application"*

*associated with the original file. You should only open files from a trustworthy source. The original file may contain executables that you may not wish to launch for security reasons.  
Do you still want to open (filename)?”*

Reply “Yes” to this message. This will open up the response in your default browser. Another message will immediately be displayed asking the following:

*“The application launched to view (filename) has exited.  
Do you wish to delete the file? If you are done with the file you can safely delete it since the original is still protected.”*

If you want to delete the unencrypted copy that is currently open select “Yes”. This action will not delete the original encrypted file and it can be opened again as long as the user is logged into Entrust. If you wish to save the unencrypted response you can say “No” and it will be in the same user directory as the encrypted file or you can do a save as and save the unencrypted file to a specified location on your PC.

## TROUBLESHOOTING

---

**Problem:** You receive an error message: “*You are not the intended recipient for this message.*” The message will not decrypt. The above error is generated.

**Solution:** You may be using the wrong Entrust account to try to decrypt the message. Only the account that is registered to the e-mail address can open the message. Please make sure you are using the correct account.

Your certificate keys may be out of sync. Contact the CMS PKI Help Desk and ask to have your keys re-synced. Once new keys have been issued, contact the State Police and ask for your responses to be re-sent to you. If re-syncing the keys does not solve the problem, the e-mail message may have been misdirected to you and you will not be able to decrypt it. Please contact the ISP Customer Service Unit at (815) 740-5160 or via e-mail at [boi\\_customer\\_support@isp.state.il.us](mailto:boi_customer_support@isp.state.il.us).

**Problem:** I am unable to open the zip file.

**Solution:** Zip files require an extractor, such as WinZip. There are several extractors on the market, as well as several free versions. WinZip has a trial version that can be used for opening zip files.

**Problem:** I need assistance with my Digital ID.

**Solution:** For questions or assistance regarding Digital ID’s, please go to the following URL: [www.illinois.gov/pki](http://www.illinois.gov/pki), select the link to “PKI FAQs”, and then select the “Who do I call for help?” topic.

**Problem:** My Digital ID has expired.

**Solution:** For an expired Digital ID password, please go to [www.illinois.gov/pki](http://www.illinois.gov/pki) and select “*Forgot Password*” from the menu to have your password reset.

**Problem:** I need assistance with the Entrust Security Provider Software.

**Solution:** For questions or assistance regarding Digital ID’s, please go to the following URL: [www.illinois.gov/pki](http://www.illinois.gov/pki), select the link to “PKI FAQs”, and then select the “Who do I call for help?” topic.

**Problem:** I received an error regarding unable to access roaming servers.

**Solution:** There are multiple reasons this can occur:

1. Insufficient privileges to install the software on the PC.
2. Some anti-virus software programs cause problems during the install. If you have AVG anti-virus software version 9.0, when installing the ESP 9.2 software choose the "Custom" option, then deselect the option to install the TrueDelete software. AVG software and the TrueDelete component are incompatible at this time.
3. Not clicking the setup.exe file to install the software; do not click the \*.msi file. Only the setup.exe file will install the configuration information for accessing the roaming servers.
4. You may have needed ports closed on your network firewalls. To test you should be able to use a telnet command to see if you can connect to us at all three of the ports that are needed. If telnet is available on your PC, you should be able to go to a DOS prompt and type the following three lines. If it connects, you will just see the prompt go to the upper left corner and flash. Pressing the escape key multiple times should get you back to a prompt. If it fails you should get a failure notice.

```
telnet servers.cmcf.state.il.us 389  
telnet roaming.cmcf.state.il.us 640  
telnet authority.cmcf.state.il.us 829
```

Normally we suggest your network group create an ACL for TCP/IP outbound only for the above port numbers (389, 640, and 829).