



Creating and processing encrypted files

This document contains some basic instructions outlining the steps required to create and execute an encrypted file on a QLn320 printer. It also briefly describes how to use the ZebraEncryptionUtility.exe developed for creating encrypted files. This utility can be obtained through your Zebra account manager or sales representative.

Note: To run 'ZebraEncryptionUtility.exe' you must have the latest Java Runtime Engine (JRE) installed.



Source File:

Specify the name and location of the file to be encrypted.

Destination File:

Specify the name and location of the output encrypted file. The file extension must be '.nre'.

Encryption Key:

Specify the name and location of a file that contains the encryption key. The file extension must be '.key'. **Note: To create a key file, select the "+" button. This will prompt for a file name where the key will be created. The key will be a random number generated by the utility. This key will be MIME encoded and written as part of a setvar command to the file name specified. This file can be sent directly to the printer for staging the encryption key.**

Include Header checkbox:

This checkbox indicates whether a 'downloadable header' should be included in the output encrypted file. If the downloadable header is included then the output encrypted file can be saved to the printer by sending the file directly via USB, serial, or as a file in the 'commands' folder of a mirror server. If the downloadable header is **not** included in the output encrypted file, then the only way to save the file on the printer is to place the file in the 'files' folder of a mirror server.

Here is an example screenshot with all three fields populated with sample data:



Contents of OPEN_TTT.txt:

```
! U1 setvar "wlan.essid" "TTT"  
! U1 setvar "wlan.encryption_mode" "off"  
! U1 setvar "wlan.wpa.enable" "off"  
! U1 setvar "wlan.leap_mode" "off"  
! U1 setvar "wlan.kerberos.mode" "off"  
! U1 setvar "wlan.8021x.enable" "off"  
! U1 setvar "wlan.operating_mode" "infrastructure"  
! U1 setvar "ip.dhcp.enable" "on"  
! U1 setvar "ip.bootp.enable" "off"  
! U1 setvar "ip.port" "6101"  
! U1 setvar "ip.pop3.enable" "off"  
! U1 do "device.reset" ""
```

When the fields described above are correctly populated, press the 'Encrypt File'. If all goes well, the following dialog should appear:



Sending the encrypted file to the printer:

After creating the encrypted file, the file must be saved on the printer. This can be done in one of two ways:

- Sending the file directly to the printer via USB, serial, TCP or mirror (commands folder). Note: this method assumes the 'Include Header' checkbox was checked when the file was encrypted.
- Placing the encrypted file in the 'files' folder of a mirror server. Note: this method assumes the 'Include Header' checkbox was **not** checked when the file was encrypted.

Staging the printer with the encryption key:

To decrypt the file, the printer must be staged with the encryption key. The key value must be MIME encoded as part of a setvar command to be saved on the printer.

As described above, to create the MIME encoded encryption key, select the “+” button next to the ‘Encryption Key’ label. This will prompt for the name of a file where the setvar command with the MIME encoded encryption key will be created. After specifying a file name, select ‘Save’ and a file containing the setvar command with a MIME encoded encryption key will be created.

Here is an example of a MIME encoded encryption key created using the “+” button described above:

```
!! U1 setvar "device.crypt.key" "GeoOKmHL/jdzV087a8eAPrVn/Ry3j+B5"
```

The printer may be staged with the encryption key in either of the following methods:

- Sending the file directly to the printer using USB, serial,
- TCP. Placing the file in the ‘commands’ folder of a mirror server.

Executing the encrypted file:

Once the printer is staged with the encryption key and the encrypted file saved in the flash file system, the encrypted file can be executed using the “! U1 setvar "file.run"” command.

Here is an example file.run command using the encrypted file ‘OPEN_TTT.NRE’ created above:

```
! U1 setvar "file.run" "OPEN_TTT.NRE"
```

Note: The filename and extension specified in the “file.run” command must be uppercase.

See Also

- For any further information, sample code and solutions or to request further content, visit the [Zebra Developer Portal](#).

Document Control

Version	Date	Description
1.0	23 rd May 2012	Initial release
2.0	2nd October 2017	Updated URLs

Disclaimer

All links and information provided within this document are correct at time of writing Created for Zebra Global ISV Program by Zebra Development Services



Copyrights

©2010 ZIH Corp. Zebra and the Zebra head graphic are registered trademarks of ZIH Corp All rights reserved. All other trademarks are the property of their respective owners.