TMK Local Injection - User Manual

V2.0.0

1. Introduction

1.1. Overview

The TMK (Terminal Master Key) Local Injection System is an application pre-installed on a dedicated **Key Injection Device** or KLD (typically a WizarPOS 1 or WizarPOS Q2/Q3 unit). This system allows payment administrators to securely inject cryptographic keys into standard payment terminals (target POS).

1.2. Key Injection Methods

The system supports three primary methods for key injection:

1. **Local Injection from Device Storage (offline deliver):** Keys are first loaded into the Key Injection Device (via manual input or from a PC) and then injected locally into the target POS.
2. **Manual Local Injection:** Key components are manually entered directly into the Key Injection Device, which then injects the derived key into the target POS.
3. **Injection Direct from PC (online deliver):** Keys are sent directly from a PC application through the Key Injection Device to the target POS in real-time. **This method is only supported on WizarPOS 1.**

2. Quick Start Guide

This guide outlines the most common workflow: **Offline Injection** using a key previously stored on the device.

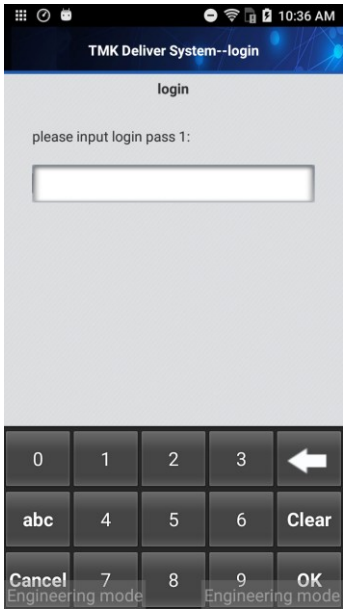
1. **Prepare the Key:** Ensure the target key is already stored on the Key Injection Device. This can be done by:
   - **Manual Input:** See Section 3.2.4 Input Key.
   - **Loading from PC:** See Section 3.3.1 Key Load
2. **Connect Devices:** Use a USB cable to connect the target POS to the appropriate port on the Key Injection Device (see Section 5 Device Connection Guide).

3. **Start Target POS KLD Agent:** On the target POS, make sure Administrator state is 'Login' (default pass: 99999999), navigate to
   System Setting -> **About POS** -> **POS Configuration** -> **Load Key**. click **Load Key**, the device will enter a waiting state.
4. **Initiate Injection:** On the Key Injection Device, from the idle screen, press **OK** to enter the Key Injection Menu. Select **Offline Deliver** and enter the deliver password (default: 00000000).
5. **Select Key:** Follow the on-screen prompts to locate the key using its identifiers (e.g., MID/TID, KSI, KID).
6. **Configure Injection:** Specify the key index (0-49) on the target POS and, for DUKPT keys, the key usage.
7. **Confirm and Inject:** Review the key information and confirm the injection. Upon success, a receipt will print, and both devices will display a success message.

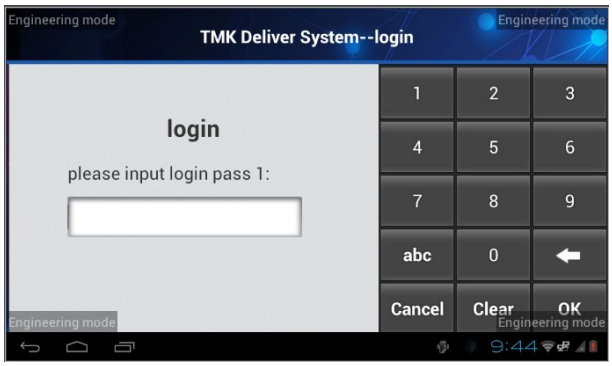
3. System Operation

3.1. Login and Idle Screen

- Upon startup, the application requires two login passwords.

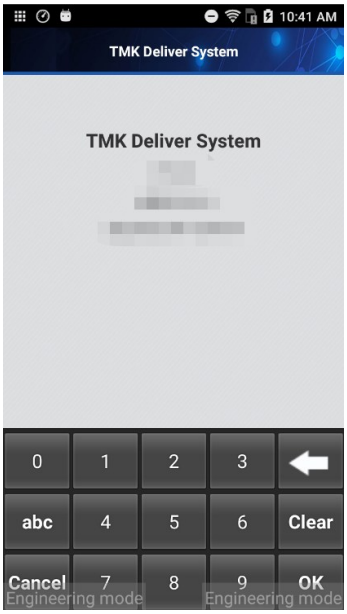


Q2/Q3

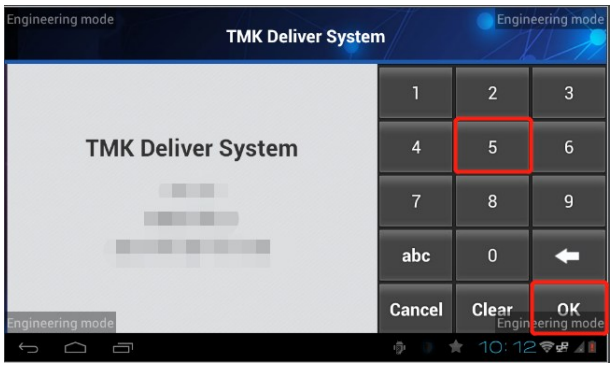


WizarPOS 1

- **Default Login Password 1:** 11111111
- **Default Login Password 2:** 22222222
- After successful authentication, the system enters the **IDLE** screen, displaying version information.

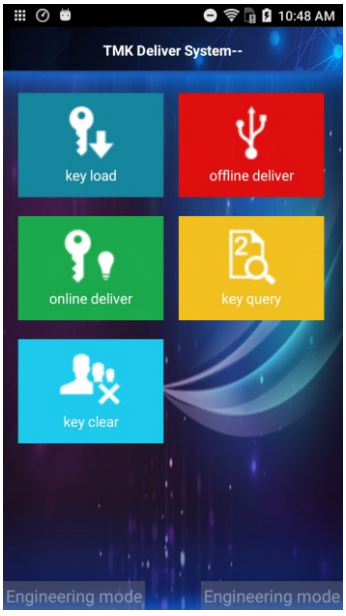


Q2/Q3 IDLE



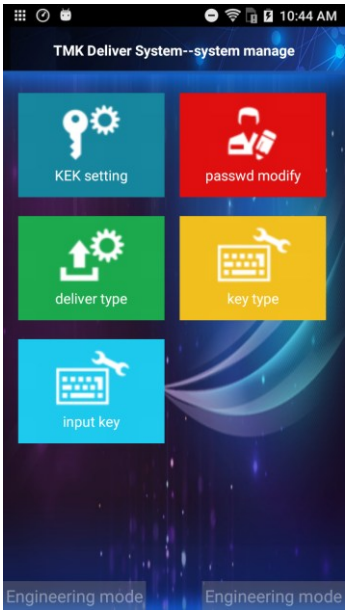
WizarPOS 1 IDLE

- From **IDLE** Screen:
  - Press **5** to enter the **System Manage** menu (default pass: **87654321**).
  - Press **OK** or **Cancel** to enter the **Key Injection** menu.

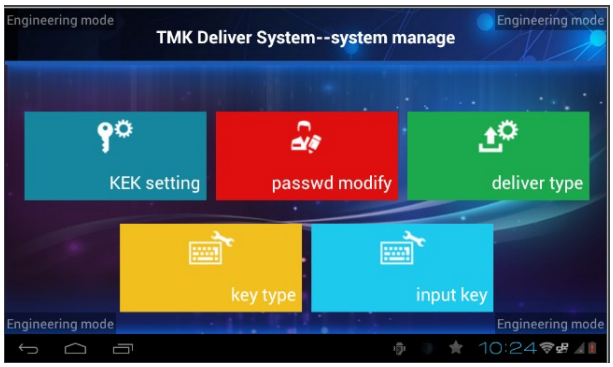


Q2/Q3 Key Injection Menu

WizarPOS 1 Key Injection Menu



Q2/Q3 system Manage



WizarPOS 1 system manage

3.2. System Management Menu

Access this menu by pressing **5** on the **IDLE** screen. The default administrator password is **87654321**.

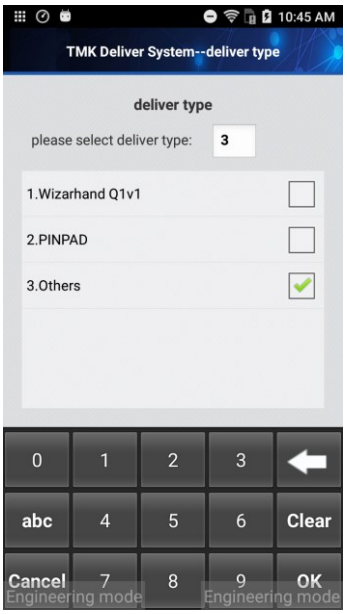
3.2.1. KEK Setting

- **Purpose:** The Key Encryption Key (KEK) is used to encrypt keys during communication with the PC or manual enter TR31 key block. It is **only required** for **Key Load**, **Online Delivery and Manul Enter TR31 Key** functions.
- **Setup:** KEK is divided into two components. Each component requires a password for setting.
    - **Default Component 1 Password:** 88888888
    - **Default Component 2 Password:** 99999999
    - **Default Component 3 Password:** 77777777
      Note: if the KEK components to be entered less than 3, keep the following component as all zero.

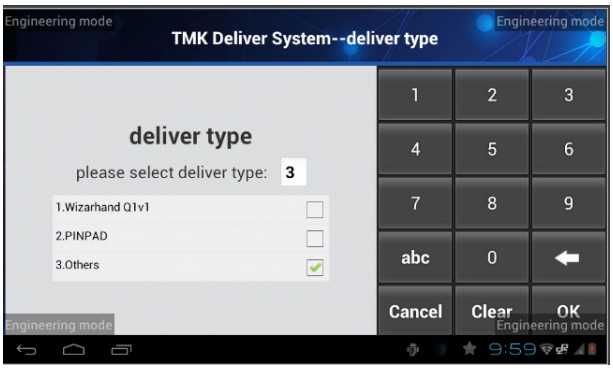
3.2.2. Deliver Type

- **Purpose:** This setting defines the model of the target POS terminal. It **must** be configured correctly before any injection attempt.
- **Options:**
    1. **Wizarhand Q1v1:** For older Q1 model terminals.

2. **PINPAD:** For external PINPAD devices.
3. **Others:** For **WizarPOS Q2, Q3**, and other modern models.



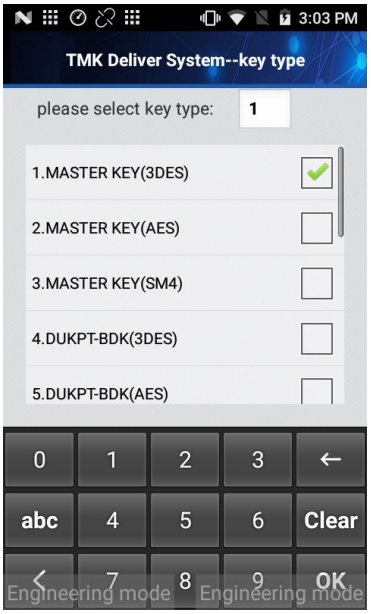
Q2/Q3



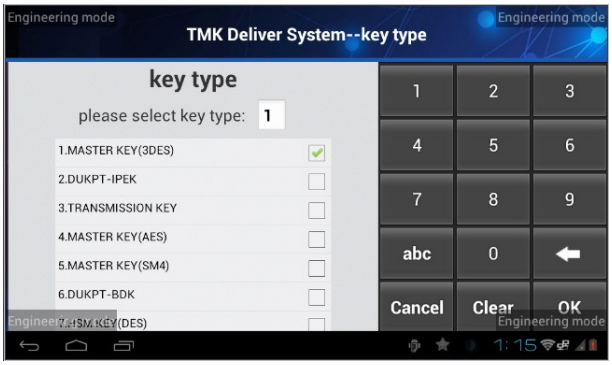
WizarPOS 1

3.2.3. Key Type

- **Purpose:** Specifies the cryptographic algorithm and type of key to be injected. This **must** be set before manually inputting a key or performing an offline injection.
- **Supported Types include:** MASTER KEY (3DES/AES/SM4), DUKPT-IPEK, DUKPT-BDK(3DES/AES), TRANSMISSION KEY(3DES/AES/SM4), HSM KEY (DES/3DES/AES/SM4).



Q2/Q3



WizarPOS 1

3.2.4. Input Key

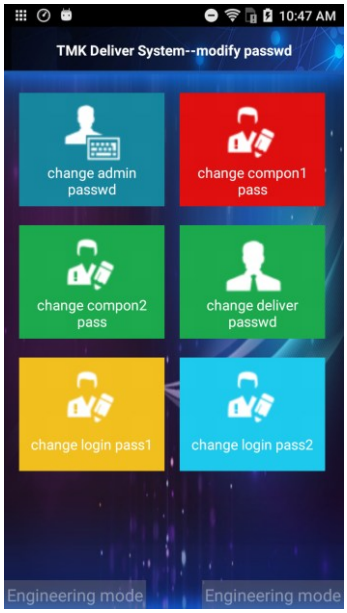
Use this function to manually enter and store a key on the device.

1. **Prerequisite:** Set the correct **Key Type** first.
2. **Enter Identifiers:** The system will prompt for specific identifiers based on the key type:
    - **MID & TID:** For MASTER KEY, DUKPT-IPEK, TRANSMISSION KEY. (Use any values if not applicable, but note them for future reference.)
    - **KSI** (First 10 digits of KSN): For DUKPT-BDK.
    - **KID** (4 digits): For all HSM KEY types.
3. **Enter Key Components:** Input the key split into its components. The system will display a check value to verify correct entry.
4. The key is now stored locally and available for **Offline Delivery**.

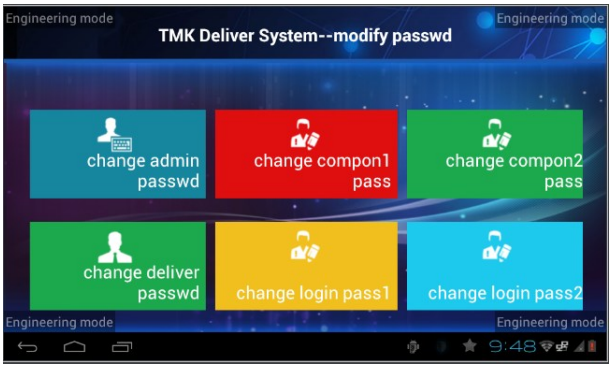
3.2.5. Password Modify

Allows changing of all system passwords:

- Administrator Password
- Deliver Password
- Login Passwords (1 & 2)
- Component Passwords



Q2/Q3



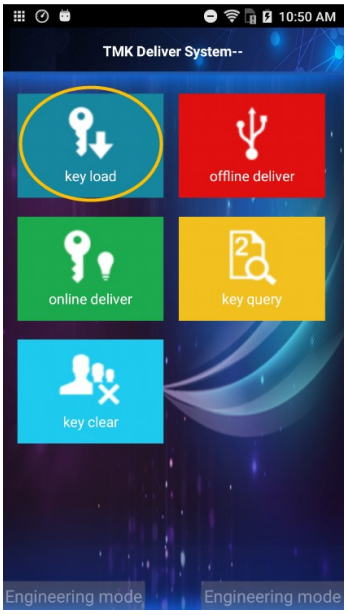
WizarPOS 1

3.3. Key Injection Menu

Access this menu by pressing **OK** or **Cancel** on the IDLE screen. The default deliver password is **00000000**.

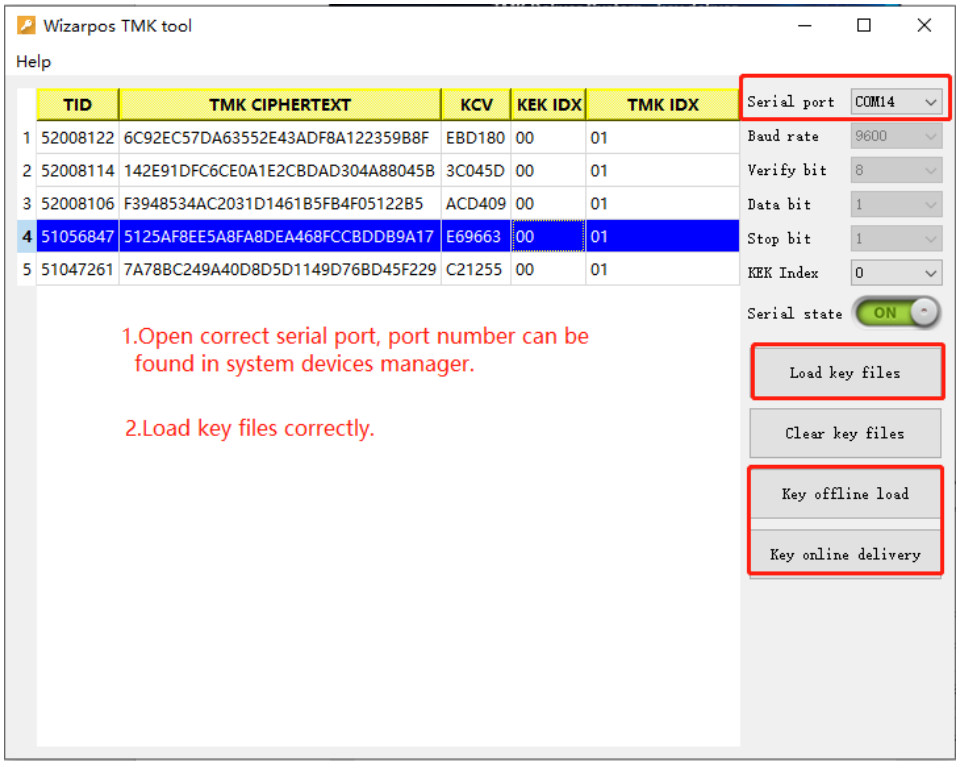
3.3.1. Key Load

- **Purpose:** Transfers keys from the PC-side Key Tool application to the Key Injection Device's local storage.
- **Prerequisite:** KEK must be set.
- **Steps:**
    1. Connect the Key Injection Device to the PC via a DB9 serial cable/USB-to-DB9 adapter (For WizarPOS 1) or USB/UU cable(For Q2,Q3).
    2. Open the Key Tool on the PC and ensure the correct serial port is selected.
    3. On the Key Injection Device, select **Key Load**. The device enters a receiving state.
    4. On the PC's Key Tool, load the key file and click **Key Offline Load** to transmit the keys.
    5. Verify the loaded keys via the **Key Query** menu.



Q2/Q3

WizarPOS 1



PC Key Tool

3.3.2. Offline Deliver

- **Purpose:** Injects a key that is already stored on the Key Injection Device (via manual input or Key Load).
- **Steps:** Refer to the detailed procedure in Section 4.1 Inject from Key Injection Device (Offline Deliver)

3.3.3. Online Deliver (WizarPOS 1 only)

- **Purpose:** Injects a key directly from the PC to the target POS in real-time, without storing it on the injection device.
- **Prerequisite:** KEK must be set.
- **Steps:** Refer to the detailed procedure in Section 4.2 Inject from PC (Online Deliver - WizarPOS 1 only)

3.3.4. Key Query

Displays a list of all keys currently stored in the local storage of the Key Injection Device.

3.3.5. Key Clear

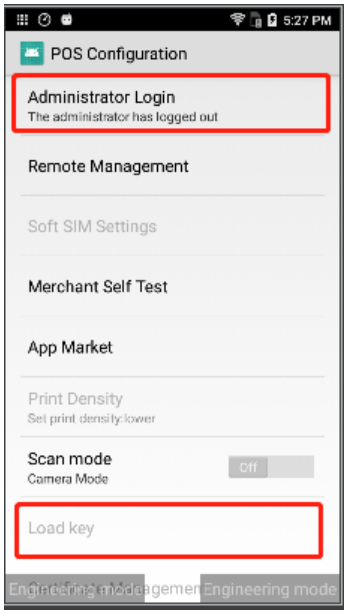
Permanently deletes all keys from the Key Injection Device's local storage.

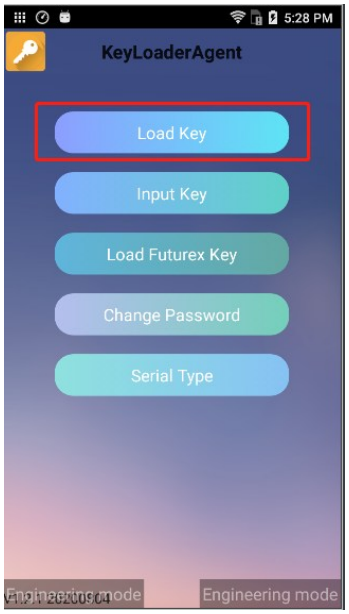
4. Detailed Key Injection Procedures

4.1. Inject from Key Injection Device (Offline Deliver)

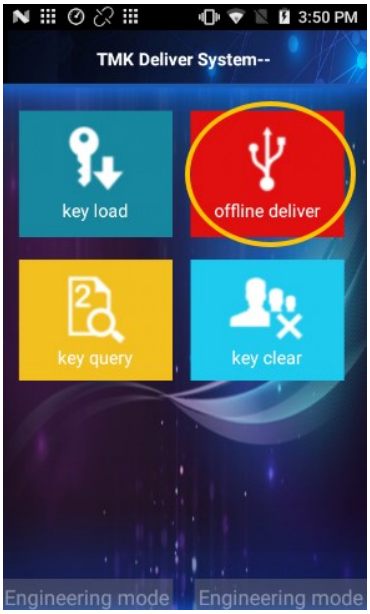
Prerequisite: Verify the key exists in the device's storage (check **Key Query**).

1. **Connectivity:** Connect the target POS to the Key Injection Device via the appropriate USB cable.
2. **Start Target Agent:** On the target POS, make sure Administrator state is 'Login' (default pass: 99999999), open the Key Loader Agent (Path: System Setting -> About POS -> POS Configuration -> Load Key). and press **Load Key** to enter a waiting state.





3. **Start Injection:** On the Key Injection Device, select **Offline Deliver** and enter the deliver password (default pass: 00000000).



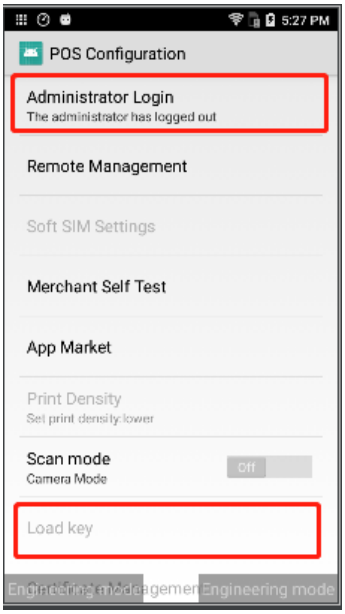
Q2/Q3

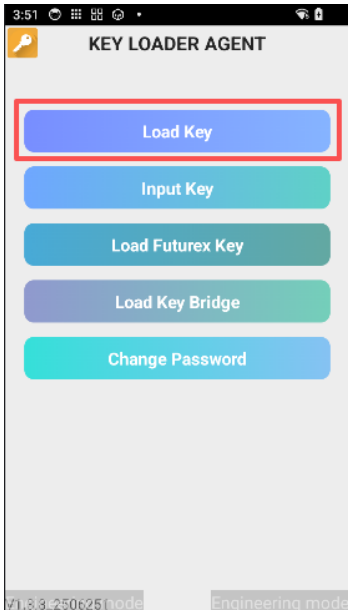
WizarPOS 1

4. **Locate Key:** Input the key's identifiers (MID/TID, KSI, or KID) as prompted to find the key.
5. **Additional Data (if applicable):**
   - For **DUKPT-BDK,** you will be prompted to enter the **DID** (part of the KSN).
   - For **DUKPT keys,** you will be prompted to select the **Key Usage** (PIN-Key, MAC-Key, Data-Key, or Reserved). Selecting Reserved allows the target HSM to derive keys per DUKPT2009 specification.
6. **Set Key Index:** Specify the key index (0-49) on the target POS's HSM where the key will be stored.
7. **Confirm and Inject:** Review all parameters and confirm to start the injection. Success will be indicated on-screen messages.

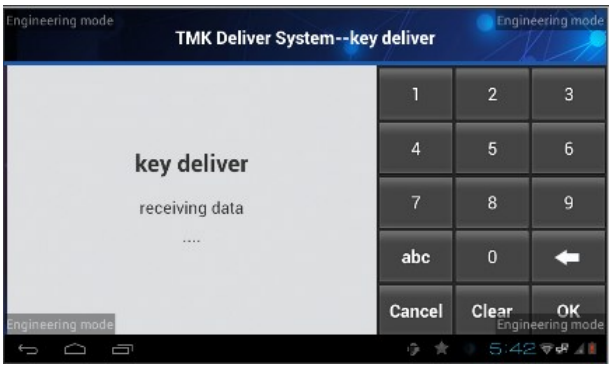
4.2. Inject from PC (Online Deliver - WizarPOS 1 only)

1. **Connectivity:** Connect the Key Injection Device to the PC via a DB9 serial cable. Connect the target POS to the Key Injection Device via a USB cable.
2. **Prerequisite:** Ensure KEK is set correctly on the Key Injection Device.
3. **Start Target Agent:** On the target POS, make sure Administrator state is 'Login' (default pass: 99999999), open the Key Loader Agent (Path: System Setting -> About POS -> POS Configuration -> Load Key). and press **Load Key** to enter a waiting state.

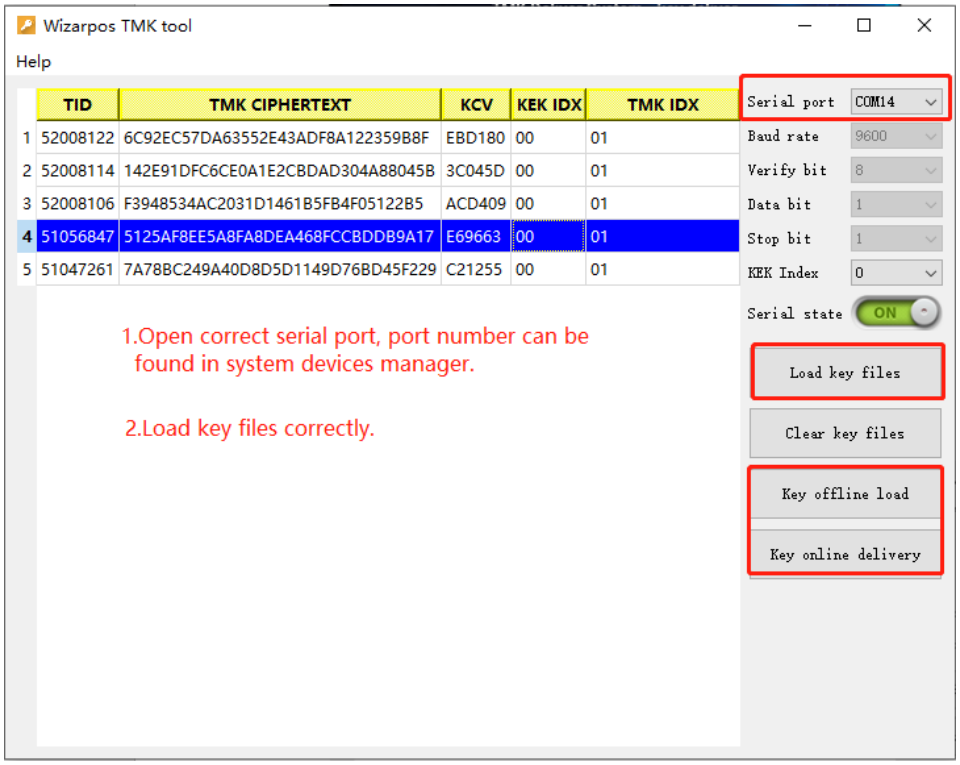




4. **Initiate Online Delivery:** On the Key Injection Device, select **Online Deliver** and enter the deliver password. The device will enter a waiting state.



5. **Send Key from PC:** On the PC's Key Tool, load the key file and use the **Key online delivery** function to send the key.



6. **Completion:** Upon successful injection, the Key Injection Device will print a receipt and display a success message. The target POS agent will also confirm success.

5. Device Connection Guide

5.1. WizarPOS Q2/Q3 as Key Injection Device

- **Connection to Target POS:** Use a USB cable connected to the **OTG/TYPE A** port.
- **Note:** The Q2/Q3 device **does not support** the **Online Delivery** functions.

5.2. WizarPOS 1 as Key Injection Device

- **Connection to Target POS:**
  - For **PINPAD:** Use an RJ11 cable connected to the **RJ11 LINE2** port.
  - For **All Other Types (Q1v1, Others):** Use a USB cable connected to the **USB TYPE A** port.
- **Connection to PC:** Use a DB9 serial cable (or USB-to-DB9 adapter) connected to the **DB9 SERIAL PORT**. Required for **Key Load** and **Online Delivery**.

6. Security and Recommended Usage

To ensure the highest level of security, adhere to the following practices:

1. **Dual Custody:** The two login passwords should be held by two different key custodians. Both custodians must be present to operate the system.
2. **Change Default Passwords Immediately:** Upon first use, change all default passwords (login, administrator, deliver, component).
3. **Compartmentalization of Knowledge:** Each key custodian should only know their own login password and key components. No single person should possess all credentials.
4. **Full-Length Components:** Each key component must be of full length, identical to the complete key length.
5. **Physical Security:** The Key Injection Device should be stored in a secure, access-controlled room and must **never** be connected to any network.
6. **Audit Logging:** Maintain a detailed log of every operation performed using the TMK Local Injection System, including date, time, custodians involved, and target terminal IDs.