RKMS Key Exchange

Version	Author	Date	Description
1.0	Lizhou	2025-06-04	The first version

1. Introduction

The document describes how users can exchange key with WizarPOS.

2. Exchange Keys

The customer can generate the key by themselves or entrust the WizarPOS to generate the key.

2.1 The customer generates the key

- The customer generates the 3 key components and KCV in security environment. The major key will be compsed by 3 key components.

- The 3 components of key should be managed by 3 key custodians in safe place.
- Each of the 3 key custodians (security officers) send his key component and its KCV to the different key custodians of WizarPOS. The key should be sealed in a security container (including pre-numbered, tamper-evident, authenticable packaging). They must be sent by different secure courier mailer
- When WizarPOS 3 key custodians (security officers) receive the 3 key components. They will combine them to HSM in secure room and check the KCVs, then upload the cipher text of key to RKMS.

2.2 WizarPOS generates the key

- There are 3 key custodians. They will generate the 3 key components and KCV in security environment. The major key will be compsed by 3 key components.
- The 3 key custodians will export the 3 key components seperately, then sending the 3 key components / KCV and the KCV of composed key to the customer seperately with 3 different courier companies
- The customer has 3 key custodians too. They will receive the 3 key components seperately and then do next process.

2.3 The 3 key custodians (security officers) of WizarPOS

Name	Email	Address
Peng Li	peng.li@wizarpos.com	1001, No.509 WuNing Rd, Shanghai,China. 200063
Caishun Duan	duancaishun@wizarpos.com	1001, No.509 WuNing Rd, Shanghai,China. 200063
Shuopeng Feng	fengshuopeng@wizarpos.com	1001, No.509 WuNing Rd, Shanghai,China. 200063

3. KEK protects working key

The working key protected by KEK should be in TR31 format. We currently support the C and D versions of TR31 format.

- The TR31 header of BDK that KEK protected

TR31 Version	C, for TDEA D, for AES
Header	B0TX, B0TN, B0DX, B0DB, B0DN

- The TR31 header of Master Key that KEK protected

TR31 Version	C, for TDEA D, for AES
Header	K1TB, K1DB