CWSE APDU Command Specification

文件編號: CW-SPEC-0002

版別(0110)

合約號碼:N/A

出版日期:2015/11/16

交付日期:N/A

製文單位: 銓安智慧科技股份有限公司

CWSE APDU (Command Spe	文件編號:		
		CW	/-SPEC-0002	
				版別(0110)
			出版日期:	2015/11/16
	銓安智慧	科技股份	有限公司	
擬訂:				
(Prepared by)				
	姓名/職稱	日期	姓名/職稱	日期
		委託方		
接收: (Received by)	姓名/職稱	日期	_	
審查: (Reviewed by)	姓名/職稱	日期		日期
	姓名/職稱	日期	姓名/職稱	日期
核定:				
(Approval by)	姓名/職稱	日期	_	

修訂紀錄

版本編號	修訂日期	修訂人	修訂內容	
0100	2014/5/7	Roy Lin	Initial draft	
0101	2014/6/14	Roy Lin	 Add the following commands: se_init_set_data se_init_get_data_hash se_init_confirm se_init_wmk_chlng se_init_back_init se_init_change_vmk se_perso_set_data se_perso_get_data_hash se_perso_back_perso se_perso_back_perso se_pin_unlock se_se_set_currency se_get_currency se_get_currency se_trx_begin se_trx_sign se_trx_status 	

			 Remove the following commands: se_puk_change se_puk_version Wallet balance: 16 bytes -> 8 bytes
			se_actv_wallet command:wallet profile: name, addr, prk
0102	2014/6/30	Roy Lin	 se_perso_back_perso: Add new pin hash setting se_pin_unlock Add new pin hash setting Responses for authentication: Hash (32 bytes) -> Encryption result (16 bytes) se_init_back_init se_init_change_vmk se_pin_auth se_pin_unlock trx_sign commands: 6xh -> 7xh
0103	2014/8/9	Roy Lin	 Add commands: se_trx_prepare se_trx_get_ctxinfo se_qry_wallet_info (Remove se_qry_wallet_balance) se_qry_wallet_info_len se_wallet_pkg_balnc se_wallet_get_map se_get_card_name

			■ se_set_card_name
			Modified commands:
			se_find_empty_wallet: WAID 1 byte -> 2 bytes, RFU parameter removed
			se_qry_wallet_id: WAID 1 byte -> 2 bytes, RFU parameter removed
			<pre>se_qry_wallet_id: wallet name hash -> wallet name</pre>
			se_actv_wallet: wallet name hash-> wallet name, WAID 1 byte ->2 bytes
			<pre>se_deactv_wallet: WAID 1 byte - > 2 bytes</pre>
			se_trx_begin: WAID 1 byte -> 2 bytes
			se_get_currency andse_set_currency: currency 1 byte> 5 bytes
			 Instruction IDs for trx signing commands are changed
			Add commands:
			■ se_actv_wallet_genkey
			■ se_get_wapkg_name
			■ se_set_wapkg_name
0104	2014/8/30	Roy Lin	• Modify commands:
			■ se_trx_get_ctxinfo:
			◆ Add IN_ID parameter
			◆ Modify INFOID
			• num_in: 1 byte -> 2 bytes

			■ se_trx_prepare: Add parameter WAID, BALANCE and HASH
			se_trx_begin: Remove parameter WAID and add parameter AMOUNT
			• Trx signing input limit: 10 -> 256
			Add commands:
			■ Backup-restore commands
			■ HDW commands
			Host binding commands
			 PINHASH is encrypted by BIND_CHAN in se_perso_back_perso and se_pin_unlock
			HASH value -> MAC value for the following commands:
			■ se_pin_change
0.1.0.5			■ se_actv_wallet
0105	2014/10/15	Roy Lin	<pre>se_qry_wallet_info</pre>
			■ se_wallet_get_map
			■ se_actv_wallet_genkey
			■ se_trx_prepare
			■ se_trx_sign
			WAPRK is encrypted by BIND_CHAN in se_actv_wallet
			 WAADDR: 32 bytes -> 25 bytes in se_actv_wallet and se_qry_wallet_info (For consistency)
			Instruction ID change:
			■ se_trx_status: 70h -> 80h

			se_bak_status: 80h -> 88h
0106	2014/11/18	Roy Lin	 se_pin_auth and se_pin_change: can be executed if PIN function is not enabled in security policy hdw_init_wallet_gen: Add parameter SEEDNUM, ACTVCODE, MAC hdw_qry_wa_info,hdw_qry_acc_info: don't need pin auth add hdw_init_wallet_gen_confirm hdw_prep_trx_sign: add parameter balance Add command: se_hdw_qry_acc_keyinfo se_set_secpo Remove HST_ID parameter in se_bind_logout
0107	2015/1/13	Roy Lin	 Remove wallet_mgmt commands Remove backup/restore commands Modified commands: se_hdw_init_wallet se_hdw_create_account se_trx_get_ctxinfo: Output info_hash -> info se_bind_find_hst_id: Only supported in NOHOST mode New commands: se_get_card_id se_xchs_reg_status se_xchs commands

			• OTP: 8 digits -> 6 digits
			■ se_bind_reg_init
			■ se_trx_begin
			■ se_xchs_get_otp
			Add command se_get_card_id
			Add card ID and XCHS SEMK in initialization data
			Add credential commands
	2015/6/29	Roy Lin	 Add init data IDs: XCHS_SEMK, CARD_ID, XCHS_OTPK, XCHS_SMK
0108			Add command se_trx_outaddr
			 Modify command se_trx_begin (Add enc_outaddr parameter)
			 ■ Binding host description: 128 bytes → 64 bytes
			Add error code list
			• Fix some typos
			Add se_get_basic_info command
0109	2015/8/14	Roy Lin	Add all_hdw_info in se_hdw_qry_wa_info command
			Add all_acc_info in se_hdw_qry_acc_info command
0110	2015/11/16	Roy Lin	Add account public key parameter in se_hdw_qry_acc_keyinfo

目 錄

修	訂紀錄		III
目	錄		IX
1.	•	ODUCTION	
2.	CWSE	APDU COMMAND LIST	2
3.	CWSE	APDU COMMAND ERROR CODES	6
4.	CWSE	APDU COMMAND SPECIFICATION	9
_		NFORMATION	
	4.1.1.	se_get_mode_state	
	4.1.2.	se_get_fw_version	
	4.1.3.	se_get_unique_id	
	4.1.4.	se_get_mod_err	12
	4.1.5.	se_get_basic_info	13
	4.1.6.	se_back_ikvldr	14
2	4.2. Init	IALIZATION	15
	4.2.1.	se_init_set_data	15
	4.2.2.	se_init_get_data_hash	16
	4.2.3.	se_init_confirm	17
	4.2.4.	se_init_vmk_chlng	18
	4.2.5.	se_init_back_init	19
	4.2.6.	se_init_change_vmk	20
2	4.3. Hos	T BINDING	21
	4.3.1.	se_bind_reg_init	21
	4.3.2.	se_bind_reg_chlng	22
	4.3.3.	se_bind_reg_finish	23
	4.3.4.	se_bind_reg_info	24
	4.3.5.	se_bind_reg_approve	25
	4.3.6.	se_bind_reg_remove	26
	4.3.7.	se_bind_login_chlng	27
	4.3.8.	se_bind_login	28
	4.3.9.	se_bind_logout	29
	4.3.10.	se_bind_find_hstid	30
	4.3.11.	se_bind_back_nohost	31

4.4.	PERS	SONALIZATION	32
4	4.4.1.	se_perso_set_data	32
4	4.4.2.	se_perso_get_data_hash	33
4	4.4.3.	se_perso_confirm	34
4	4.4.4.	se_perso_back_perso	35
4.5.	AUT	HENTICATION	36
4	1.5.1.	se_pin_chlng	36
4	1.5.2.	se_pin_auth	37
4	1.5.3.	se_pin_change	38
4	1.5.4.	se_pin_logout	39
4	1.5.5.	se_puk_chlng	40
4	1.5.6.	se_pin_unlock	41
4.6.	BCD	OC SETTING	42
4	4.6.1.	se_set_currency	42
4	4.6.2.	se_get_currency	43
4	4.6.3.	se_get_card_name	44
4	4.6.4.	se_set_card_name	45
4	4.6.5.	se_get_secpo	46
4	4.6.6.	se_set_secpo	47
4	4.6.7.	se_get_card_id	48
4.7.	TRA	NSACTION SIGNING	49
4	1.7.1.	se_trx_status	49
4	1.7.2.	se_trx_begin	50
4	1.7.3.	se_trx_verify_otp	51
4	1.7.4.	se_trx_sign	52
4	1.7.5.	se_trx_get_ctxinfo	53
4	4.7.6.	se_trx_finish	54
4	1.7.7.	se_trx_outaddr	55
4.9.	HD	Wallet	56
4	2.9.1.	se_hdw_init_wallet	56
4	.9.2.	se_hdw_init_wallet_gen	57
4	1.9.3.	se_hdw_qry_wa_info	58
4	.9.4.	se_hdw_set_wa_info	59
4	.9.5.	se_hdw_create_account	60
4	9.6.	se_hdw_qry_acc_info	61
4	4.9.7.	se_hdw_set_acc _info	62

	4.9.8.	se_hdw_next_trx_addr	63
	4.9.9.	se_hdw_prep_trx_sign	64
	4.9.10.	se_hdw_init_wallet_gen_confirm	65
	4.9.11.	se_hdw_qry_acc_keyinfo	<u>66</u>
	4.10. MAII	BOX	67
	4.10.1.	mbox_spi_get_msg	67
	4.10.2.	mbox_spi_send_resp	68
	4.10.3.	mbox_iso_send_msg	69
	4.10.4.	mbox_iso_get_resp	70
	4.11. EXCH	HANGE SITE	71
	4.11.1.	se_xchs_reg_status	71
	4.11.2.	se_xchs_reg_init	72
	4.11.3.	se_xchs_reg_finish	73
	4.11.4.	se_xchs_reg_clear	74
	4.11.5.	se_xchs_get_otp	75
	4.11.6.	se_xchs_session_init	76
	4.11.7.	se_xchs_session_estab	77
	4.11.8.	se_xchs_session_logout	78
	4.11.9.	se_xchs_block_info	79
	4.11.10.	se_xchs_block_btc	80
	4.11.11.	se_xchs_cancel_block	82
	4.11.12.	se_xchs_trxsign_login	84
	4.11.13.	se_xchs_trxsign_prepare	85
	4.11.14.	se_xchs_trxsign_logout	86
	4.12. CREE	DENTIAL	87
	4.12.1.	se_cred_get_mem	87
	4.12.2.	se_cred_set_mem	88
	4.12.3.	se_cred_get_nvm	89
	4.12.4.	se_cred_set_nvm	90
5.	SUPP0	ORTED COMMANDS IN EACH MODE	
	5.1. APD	U IN EACH MODE – ISO INTERFACE	91
		U IN EACH MODE – SPI INTERFACE	

1. Introduction

SE (Secure Element) is cryptographic engine and secure storage of key and data for BCDC. It provides ISO and SPI communication interface. For SPI interface introduction, please refer to "*BCDC SE SPI Slave User Manual*". This documents list all supported APDU commands and specifications of them in ISO and SPI interface.

2. CWSE APDU Command List

Category: SE Info						
Command	INS	SPI	ISO	Descriptions		
se_get_mode_state	10	V	V	Get SE mode and state		
se_get_fw_version	11	V	V	Get SE firmware version		
se_get_unique_id	12	V	V	Get SE unique ID		
se_get_mod_err	13	V	V	Get internal module error		
se_get_basic_info	14	V	V	Get SE basic info		
se_back_ikvldr	78	V	V	Back to IKV loader		
		Cate	gory:	Init		
Command	INS	SPI	ISO	Descriptions		
se_init_set_data	A0	V	V	Set init data		
se_init_get_data_hash	A1	V	V	Get init data hash		
se_init_confirm	A2	V	V	Confirm init data		
se_init_vmk_chlng	A3	V	V	Get VMK challenge		
se_init_back_init	A4	V	V	Back to INIT state		
se_init_change_vmk	A5	V	V	Change VMK		
	Cat	egory	Host	Binding		
Command	INS	SPI	ISO	Descriptions		
se_bind_reg_init	D0	V	V	Init binding registeration		
se_bind_reg_chlng	D1	V	V	Get registration challenge		
se_bind_reg_finish	D2	V	V	Finish binding registration		
se_bind_reg_info	D3	V	V	Get registered host info		
se_bind_reg_approve	D4	V	V	Approve registered host		
se_bind_reg_remove	D5	V	V	Remove registered host		
se_bind_login_chlng	D6	V	V	Binding login challenge		
se_bind_login	D7	V	V	Host binding login		
se_bind_logout	D8	V	V	Host binding logout		
se_bind_find_hstid	D9	V	V	Find host ID by credential		
se_bind_back_nohost	DA	V	V	Back to no host mode		
Category: Perso						
Command	INS	SPI	ISO	Descriptions		
se_perso_set_data	30	V	V	Set perso data		

se_perso_get_data_hash	31	V	V	Get perso data hash			
se_perso_confirm	32	V	V	Confirm perso data			
se_perso_back_perso	33	V	V	Back to PERSO state			
Category: Auth							
Command	INS	SPI	ISO	Descriptions			
se_pin_chlng	20	V	V	Get PIN auth challenge			
se_pin_auth	21	V	V	PIN authentication			
se_pin_change	22	V	V	Change PIN			
se_pin_logout	23	V	V	PIN logout			
se_puk_chlng	24	V	V	Get PUK challenge			
se_pin_unlock	25	V	V	Unlock PIN by PUK			
	Cate	egory:	BCD	C Setting			
Command	INS	SPI	ISO	Descriptions			
se_set_currency	40	V	V	Set currency setting			
se_get_currency	41	V	V	Get currency setting			
se_get_card_name	42	V	V	Get SE card name			
se_set_card_name	43	V	V	Set SE card name			
se_get_secpo	44	V	V	Get security policy setting			
se_set_secpo	45	V	V	Set security policy setting			
se_get_card_id	46	V	V	Get SE card ID			
	Ca	tegory	: Trx	Signing			
Command	INS	SPI	ISO	Descriptions			
se_trx_status	80	V	V	Get transaction signing status			
se_trx_prepare	71	V	V	Prepare Trx signing			
se_trx_begin	72	V	V	Transaction signing begins			
se_trx_verify_otp	73	V	V	Verify OTP			
se_trx_sign	74	V	V	Sign transaction			
se_trx_get_ctxinfo	75	V	V	Get transaction signing context info			
se_trx_finish	76	V	V	Finish transaction signing			
se_trx_outaddr	79	V		Get trx signing output address			
Category: HDW							
Command	INS	SPI	ISO	Descriptions			
se_hdw_init_wallet	В0	V	V	Initialize HDW			
se_hdw_init_wallet_gen	B1	V	V	Initialize HDW (gen key)			
se_hdw_qry_wa_info	B2	V	V	Query HDW info			

se_hdw_set_wa_info	В3	V	V	Set HDW info		
se_hdw_create_account	B4	V	V	Create HDW account		
se_hdw_qry_acc_info	B5	V	V	Query HDW account info		
se_hdw_set_acc_info	В6	V	V	Set HDW account info		
se_hdw_next_trx_addr	B7	V	V	Get next trx address		
se_hdw_prep_trx_sign	В8	V	V	Prepare HDW trx signing		
se_hdw_init_wallet_gen_confirm	В9	V	V	Confirm HDW initialization (gen key)		
se_hdw_qry_acc_keyinfo	BA	V	V	Query HDW account key info		
	C	atego	ry: Ma	ailbox		
Command	INS	SPI	ISO	Descriptions		
mbox_spi_get_msg	E0	V		Get mailbox message		
mbox_spi_send_resp	E1	V		Send response to mailbox		
mbox_iso_send_msg	E8		V	Send mailbox message		
mbox_iso_get_resp	E9		V	Get response to mailbox		
Category: Exchange Site						
Command	INS	SPI	ISO	Descriptions		
se_xchs_reg_status	F0	V	V	Get registration status		
se_xchs_reg_init	F1	V	V	Registration init		
se_xchs_reg_finish	F2	V	V	Registration finish		
se_xchs_reg_clear	F3	V	V	Clear registration status		
se_xchs_get_otp	F4	V	V	Get exchange site OTP		
se_xchs_session_init	F5	V	V	Exchange site session init		
se_xchs_session_estab	F6	V	V	Exchange site session establish		
se_xchs_session_logout	F7	V	V	Logout established session		
se_xchs_block_info	F8	V	V	Get blocking info		
se_xchs_block_btc	F9	V	V	Block account Bitcoin		
se_xchs_cancel_block	FA	V	V	Cancel Bitcoin blocking		
se_xchs_trxsign_login	FB	V	V	Exchange site trx signing login		
se_xchs_trxsign_prepare	FC	V	V	Exchange site trx signing prepare		
se_xchs_trxsign_logout	FD	V	V	Exchange site trx signing logout		
Category: Credential						
Command	INS	SPI	ISO	Descriptions		
se_cred_get_mem	38	V	V	Get memory credential		
se_cred_set_mem	39	V	V	Restore memory credential		
se_cred_get_nvm	3A	V	V	Get NVM credential		

se_cred_set_nvm	3B	V	V	Restore NVM credential

3. CWSE APDU Command Error Codes

Error ID (Hex)	Error Code	Description
01	ERR_CMD_NOT_SUPPORT	Command not supported
02	ERR_MODE_ID	Wrong mode ID
03	ERR_LC	Wrong APDU LC
04	ERR_TEST_FUNC_ID	Wrong test function ID
05	ERR_BCDC_TRX_STATE	Wrong trx signing state
06	ERR_TRX_VERIFY_OTP	Trx OTP verification fail
07	ERR_WALLET_INACTIVE	Wallet is not active
08	ERR_WALLET_ACTIVE	Wallet is active
09	ERR_WALLET_MISMATCH	Wallet id mismatch
0A	ERR_WRONG_OUTID	Wrong output id for trx_sign
0B	ERR_CDATA_TIMEOUT	Waiting for cdata timeout (7816 interface only)
0C	ERR_NO_RESP	No response data (7816 interface only)
0D	ERR_HASH_CHECK	Fail to pass hash check
0E	ERR_WAADDR_CHECK	Fail to pass wallet address check
0F	ERR_BCDC_INITSTATE	Wrong BCDC init state
10	ERR_BCDC_IDATAINFO	Wrong input init data information
11	ERR_BCDC_IDATASTATE	Wrong init data state
12	ERR_BCDC_PERSOSTATE	Wrong BCDC perso state
13	ERR_BCDC_PDATAINFO	Wrong input perso data information
14	ERR_BCDC_PDATASTATE	Wrong perso data state
15	ERR_DRNG_GEN_RAND	DRNG module failed to generate random bytes
16	ERR_BCDC_TRX_INID	Wrong input ID
17	ERR_NO_CHLNG	No auth challenge generated
18	ERR_LOCK	Auth locked
19	ERR_AUTHFAIL	Auth fail, not locked yet
1A	ERR_AUTHLOCK	Auth fail and locked
1B	ERR_NO_AUTH	Not authed yet
1C	ERR_NO_LOCK	Not locked

1E ERR_NO_CARDNAME No card name exists 1F ERR WALLET_ID Wrong wallet ID 20 ERR EWAINFO_ID Wrong export wallet info ID 21 ERR_NO_CURRENCY No currency data exists 22 ERR_TRX_INFOID Wrong trx context INFO ID 23 ERR_WAPKG_ID Wrong wallet package ID 24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA STATUS Wrong wallet status 28 ERR_RES_CHKSUM Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_ANDLE Wrong restore handle 2B ERR_RES_RES_HANDLE Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGIN Not in binding login state 2E ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong host login status 32 ERR_HDW_NULEN Wrong humber set length 33 ERR_HDW_NULEN Wrong HDW account ID 34 ERR_HDW_NFOID Wrong HDW account ID 35 ERR_HDW_ACCID Wrong key chain ID 36 ERR_HDW_ACCID Wrong key chain ID 37 ERR_HDW_ACCID Wrong key chain ID 38 ERR_HDW_ACCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account pointer value 42 ERR_BIND_LOGINST Wrong account pointer value 44 ERR_BIND_LOGINST Wrong account pointer value 45 ERR_BIND_LOGINST FULL. Full of hosts	1D	ERR TEST SUBFUNC ID	Wrong test sub-function ID
1F ERR_WALLET_ID Wrong wallet ID 20 ERR_EWAINFO_ID Wrong export wallet info ID 21 ERR_NO_CURRENCY No currency data exists 22 ERR_TRX_INFOID Wrong trx context INFO ID 23 ERR_WAPKG_ID Wrong wallet package ID 24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_LOGINSTAT Wrong host binding status 2F ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong humber set length 33 ERR_HDW_STATUS Wrong HDW info ID 34 ERR_HDW_INFOID Wrong HDW info ID 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_ACCID Wrong key chain ID 38 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account pointer value 42 ERR_HDW_ACCINFOLEN Wrong account pointer value 44 ERR_BIND_LIRRST Wrong first flag	1E		-
20 ERR_EWAINFO_ID Wrong export wallet info ID 21 ERR_NO_CURRENCY No currency data exists 22 ERR_TRX_INFOID Wrong trx context INFO ID 23 ERR_WAPKG_ID Wrong wallet package ID 24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong wallet status 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 20 ERR_RES_HANDLE Wrong restore handle 21 ERR_RES_HANDLE Wrong restore seed ID 22 ERR_RES_BID Wrong restore seed ID 23 ERR_BIND_HSTID Wrong binding host ID 24 ERR_BIND_HSTID Wrong binding login state 25 ERR_BIND_LOGINN Not in binding login state 26 ERR_BIND_LOGINSTAT Wrong host binding status 27 ERR_BIND_LOGINSTAT Wrong host binding status 28 ERR_BIND_LOGIN Binding login fail 30 ERR_BIND_LOGIN Wrong HD wallet status 30 ERR_BIND_LOGIN Wrong HDW wife ID 31 ERR_HDW_STATUS Wrong HDW info ID 32 ERR_HDW_INFOID Wrong HDW info ID 33 ERR_HDW_INFOLEN Wrong HDW info length 34 ERR_HDW_ACCID Wrong HDW account ID 35 ERR_HDW_ACCID Wrong HDW account info ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_ACCINFOID Wrong key ID 38 ERR_HDW_ACCINFOID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCIPTE Wrong account info length 41 ERR_HDW_ACCIPTER Wrong account info length 42 ERR_HDW_ACCIPTE Wrong account info length 44 ERR_BIND_FIRST Wrong first flag	1F		Wrong wallet ID
21 ERR_NO_CURRENCY No currency data exists 22 ERR_TRX_INFOID Wrong trx context INFO ID 23 ERR_WAPKG_ID Wrong wallet package ID 24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong wallet status 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOID Wrong HDW info ID 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KYID Wrong key ID 39 ERR_HDW_ACTYCODE Wrong account info length 40 ERR_HDW_ACCYTR Wrong account pointer value 42 ERR_BIND_LARDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	20		
22 ERR_TRX_INFOID Wrong trx context INFO ID 23 ERR_WAPKG_ID Wrong wallet package ID 24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 20 ERR_RES_HANDLE Wrong restore checksum 21 ERR_RES_HANDLE Wrong restore seed ID 22 ERR_BIND_HSTID Wrong binding host ID 23 ERR_BIND_HSTSTAT Wrong host binding status 24 ERR_BIND_HSTSTAT Wrong host binding status 25 ERR_BIND_LOGINSTAT Wrong host login state 26 ERR_BIND_LOGINSTAT Wrong host login status 27 ERR_BIND_LOGIN Binding login fail 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong humber set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOID Wrong HDW info ID 35 ERR_HDW_ACCINFOID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KYID Wrong key ID 38 ERR_HDW_KYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 41 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_LARDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	21	ERR NO CURRENCY	
24 ERR_INTER_MODULE Internal module error 25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong HDW info ID 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCIVED Wrong account info length 41 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	22		
25 ERR_BAK_STATE Wrong backup status 26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOID Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account pointer value 40 ERR_HDW_ACCPTR Wrong account pointer value 41 ERR_BIND_LIRST Wrong first flag	23	ERR_WAPKG_ID	Wrong wallet package ID
26 ERR_BAK_HANDLE Wrong backup handle 27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_HSTSTAT Wrong host binding status 2E ERR_BIND_LOGIN Not in binding login state 2E ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account pointer value 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	24	ERR_INTER_MODULE	Internal module error
27 ERR_WA_STATUS Wrong wallet status 28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account ID 37 ERR_HDW_KCID Wrong HDW account info ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 41 ERR_HDW_ACCITRE Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	25	ERR_BAK_STATE	Wrong backup status
28 ERR_RES_STATE Wrong restore status 29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 41 ERR_HDW_ACCIPF 42 ERR_HDW_ACCIPF 43 ERR_HDW_OUTOFKEY Out of keys 44 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	26	ERR_BAK_HANDLE	Wrong backup handle
29 ERR_RES_CHKSUM Wrong restore checksum 2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong HDW account info ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_FIRST Wrong first flag	27	ERR_WA_STATUS	Wrong wallet status
2A ERR_RES_HANDLE Wrong restore handle 2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key Chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCYTR Wrong account pointer value 41 ERR_HDW_ACCYTR Wrong account pointer value 42 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	28	ERR_RES_STATE	Wrong restore status
2B ERR_RES_RSID Wrong restore seed ID 2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOID Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACCINFOLEN Wrong account info length 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	29	ERR_RES_CHKSUM	Wrong restore checksum
2C ERR_BIND_HSTID Wrong binding host ID 2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong HDW account info ID 38 ERR_HDW_KCID Wrong key chain ID 39 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong account pointer value 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2A	ERR_RES_HANDLE	Wrong restore handle
2D ERR_BIND_NOLOGIN Not in binding login state 2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW account ID 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong account info length 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2B	ERR_RES_RSID	Wrong restore seed ID
2E ERR_BIND_HSTSTAT Wrong host binding status 2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong account pointer value 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2C	ERR_BIND_HSTID	Wrong binding host ID
2F ERR_BIND_LOGINSTAT Wrong host login status 30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KCID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong account info length 41 ERR_HDW_ACCTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2D	ERR_BIND_NOLOGIN	Not in binding login state
30 ERR_BIND_LOGIN Binding login fail 31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACTVCODE Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2E	ERR_BIND_HSTSTAT	Wrong host binding status
31 ERR_HDW_STATUS Wrong HD wallet status 32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW account ID 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	2F	ERR_BIND_LOGINSTAT	Wrong host login status
32 ERR_HDW_NULEN Wrong number set length 33 ERR_HDW_INFOID Wrong HDW info ID 34 ERR_HDW_INFOLEN Wrong HDW info length 35 ERR_HDW_ACCID Wrong HDW account ID 36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	30	ERR_BIND_LOGIN	Binding login fail
33ERR_HDW_INFOIDWrong HDW info ID34ERR_HDW_INFOLENWrong HDW info length35ERR_HDW_ACCIDWrong HDW account ID36ERR_HDW_ACCINFOIDWrong HDW account info ID37ERR_HDW_KCIDWrong key chain ID38ERR_HDW_KEYIDWrong key ID39ERR_HDW_ACCINFOLENWrong account info length40ERR_HDW_ACTVCODEWrong activation code41ERR_HDW_ACCPTRWrong account pointer value42ERR_HDW_OUTOFKEYOut of keys43ERR_BIND_ALRDYNOHOSTAlready no host44ERR_BIND_FIRSTWrong first flag	31	ERR_HDW_STATUS	Wrong HD wallet status
34ERR_HDW_INFOLENWrong HDW info length35ERR_HDW_ACCIDWrong HDW account ID36ERR_HDW_ACCINFOIDWrong HDW account info ID37ERR_HDW_KCIDWrong key chain ID38ERR_HDW_KEYIDWrong key ID39ERR_HDW_ACCINFOLENWrong account info length40ERR_HDW_ACTVCODEWrong activation code41ERR_HDW_ACCPTRWrong account pointer value42ERR_HDW_OUTOFKEYOut of keys43ERR_BIND_ALRDYNOHOSTAlready no host44ERR_BIND_FIRSTWrong first flag	32	ERR_HDW_NULEN	Wrong number set length
34ERR_HDW_INFOLENWrong HDW info length35ERR_HDW_ACCIDWrong HDW account ID36ERR_HDW_ACCINFOIDWrong HDW account info ID37ERR_HDW_KCIDWrong key chain ID38ERR_HDW_KEYIDWrong key ID39ERR_HDW_ACCINFOLENWrong account info length40ERR_HDW_ACTVCODEWrong activation code41ERR_HDW_ACCPTRWrong account pointer value42ERR_HDW_OUTOFKEYOut of keys43ERR_BIND_ALRDYNOHOSTAlready no host44ERR_BIND_FIRSTWrong first flag	33	ERR_HDW_INFOID	Wrong HDW info ID
36 ERR_HDW_ACCINFOID Wrong HDW account info ID 37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	34		Wrong HDW info length
37 ERR_HDW_KCID Wrong key chain ID 38 ERR_HDW_KEYID Wrong key ID 39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	35	ERR_HDW_ACCID	Wrong HDW account ID
38ERR_HDW_KEYIDWrong key ID39ERR_HDW_ACCINFOLENWrong account info length40ERR_HDW_ACTVCODEWrong activation code41ERR_HDW_ACCPTRWrong account pointer value42ERR_HDW_OUTOFKEYOut of keys43ERR_BIND_ALRDYNOHOSTAlready no host44ERR_BIND_FIRSTWrong first flag	36	ERR_HDW_ACCINFOID	Wrong HDW account info ID
39 ERR_HDW_ACCINFOLEN Wrong account info length 40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	37	ERR_HDW_KCID	Wrong key chain ID
40 ERR_HDW_ACTVCODE Wrong activation code 41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	38	ERR_HDW_KEYID	Wrong key ID
41 ERR_HDW_ACCPTR Wrong account pointer value 42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	39	ERR_HDW_ACCINFOLEN	Wrong account info length
42 ERR_HDW_OUTOFKEY Out of keys 43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	40	ERR_HDW_ACTVCODE	Wrong activation code
43 ERR_BIND_ALRDYNOHOST Already no host 44 ERR_BIND_FIRST Wrong first flag	41	ERR_HDW_ACCPTR	Wrong account pointer value
44 ERR_BIND_FIRST Wrong first flag	42	ERR_HDW_OUTOFKEY	Out of keys
	43	ERR_BIND_ALRDYNOHOST	Already no host
45 ERR_BIND_HOSTFULL Full of hosts	44	ERR_BIND_FIRST	Wrong first flag
	45	ERR_BIND_HOSTFULL	Full of hosts

46	ERR_BIND_REGSTAT	Wrong host registration status
47	ERR_BIND_BRHANDLE	Wrong brhandle
48	ERR_BIND_REGRESP	Wrong registration response
49	ERR_LDR_AUTH	Back IKV loader auth fail
4A	ERR_LDR_BACK	Fail to back to IKV loader
4B	ERR_XCHS_REGST	Wrong XCHS registration status
4C	ERR_XCHS_SESSST	Wrong session status
4D	ERR_XCHS_SVRRESP	Wrong server response
4E	ERR_XCHS_OKTKN	Wrong OK token
4F	ERR_XCHS_MAC	Wrong XCHS MAC value
50	ERR_XCHS_BIFULL	XCHS block info full
51	ERR_XCHS_BLKAMNT	Wrong XCHS block amount
52	ERR_CRED_HANDLE	Wrong credential handle
53	ERR_HDW_NUCHKSUM	Wrong number set checksum
54	ERR_MAC	Wrong MAC value
55	ERR_INIT_PRID	Wrong pre-reg host ID
56	ERR_NVM_READ	Fail to perform NVM read
57	ERR_NVM_WRITE	Fail to perform NVM write
58	ERR_TRX_AMOUNT	Wrong trx amount
59	ERR_TRX_SIGTYPE	Wrong trx signature type

4. CWSE APDU Command Specification

4.1.SE Information

4.1.1. se_get_mode_state

Command	se_get_mode	e_state						
Description	Get SE mode	Get SE mode and state						
Supported Interfaces	ISO, SPI							
Supported Modes	All modes	All modes						
Command	APDU	80 10 00 00	LC	00	LE	02		
	CDATA	None						
Specification	RESPONSE	[MODE] [STA	TE] [S	W (2 by	rtes)]			
Parameter	MODE	Current MOD: 00h: INIT 01h: PERSO 02h: NORMA 03h: AUTH 04h: LOCK 05h: ERROR 06h: NOHOST 07h: DISCON	L Γ	byte)				
	STATE	Execution reus	slt of las	st comn	nand (1	byte)		
Note	None							

4.1.2. se_get_fw_version

Command	se_get_fw_v	se_get_fw_version				
Description	Get SE firms	ware version				
Supported	ISO, SPI					
Interfaces	150, 511					
Supported	All modes					
Modes	All illoues					
Command	APDU	80 11 00 00	LC	00	LE	10
<u> </u>	CDATA	None				
Specification	RESPONSE	[VERINFO] [SW (2 t	ytes)]		
Parameter	VERINFO	Version info (1	Version info (16 bytes)			
Note	None					

4.1.3. se_get_unique_id

Command	se_get_uniqu	se_get_unique_id				
Description	Get SE unique	ue ID				
Supported	ISO, SPI					
Interfaces	150, 511					
Supported	All modes					
Modes	All illoues					
Command	APDU	80 12 00 00	LC	00	LE	08
0 0 1111111111	CDATA	None				
Specification	RESPONSE	[UID] [SW (2	[UID] [SW (2 bytes)]			
Parameter	UID	Unique ID (81	Unique ID (8 bytes)			
Note	None					

4.1.4. se_get_mod_err

Command	se_get_mod	_err					
Description	Get internal	module error					
Supported	ISO, SPI						
Interfaces	130, 311						
Supported	All modes						
Modes	All liloues	All modes					
Cammand	APDU	80 13 00 00	LC	00	LE	02	
Command	CDATA	None					
Specification	RESPONSE	[MODID] [MO	ODERR	R] [SW	(2 bytes)]	
Parameter	MODID	Module ID (2 bytes, little-endian)					
Parameter	MODERR	Module error ((6 bytes	, little-e	endian)		
Note	None						

4.1.5. se_get_basic_info

Command	se_get_basic	_info					
Description	Get SE basic info						
Supported							
Interfaces	150, SP1	ISO, SPI					
Supported	All modes						
Modes	All illoues						
	APDU	80 14 00 00	LC	00	LE	22	
Command	CDATA	None					
Specification	RESPONSE	[MODE] [STA	TE] [V	ERINF	O] [UII)]	
		[CARDID] [S	W (2 by	rtes)]			
		Current MOD	E ID (1	byte)			
		00h: INIT					
		01h: PERSO					
		02h: NORMAL					
	MODE	03h: AUTH					
		04h: LOCK					
Parameter		05h: ERROR					
		06h: NOHOS	Γ				
		07h: DISCONN					
	STATE	Execution reus	slt of la	st comn	nand (1	byte)	
	VERINFO	Version info (1	6 bytes	s)			
	UID	Unique ID (81	oytes)				
	CARDID	Card ID (8 byt	tes)				
Note	Card ID field	d is 00h's if SE	is not ii	nitialize	ed yet		

4.1.6. se_back_ikvldr

Command	se_back_ikv	ldr				
Description	Back to IKV	loader				
Supported	ISO, SPI					
Interfaces	150, 511					
Supported	All modes					
Modes	All liloues					
Command	APDU	80 78 00 00	LC	10	LE	00
	CDATA	[BLOTP]				
Specification	RESPONSE	[SW (2 bytes)]]			
Parameter	BLOTP	Back loader O	Back loader OTP (16 bytes)			
Note	None					

4.2.Initialization

4.2.1. se_init_set_data

Command	se_init_set_o	lata				
Description	Set init data					
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	00h: INIT					
Modes	UUII. IINI I					
Command	APDU	80 A0 [IDID] [PRID]	LC	var.	LE	00
Specification	CDATA	[INITDATA] [IDHASH]				
Specification	RESPONSE	[SW (2 bytes)]				
Parameter	IDID	Init data ID 0: Default User PIN 1: PUK (32 bytes) 2: SEMK (32 bytes) 3: Card ID (8 bytes) 4: OTPK (32 bytes) 5: SMK (32 bytes) 6: Pre-reg host desc 7: Pre-reg host OTI))) cription	n (64 b	ytes)	
	PRID	Pre-reg host ID (0 of Only used for IDID		17		
	INITDATA	Init data (variable l	ength)			
	IDHASH	SHA256 value of I	NITD	ATA (3	2 byte	s)
Note	None			-		

4.2.2. se_init_get_data_hash

Command	se_init_get_	data_hash						
Description	Get init data	Get init data hash						
Supported	ISO, SPI	SO SPI						
Interfaces	150, 511	50, 511						
Supported	00h: INIT							
Modes	0011. 11 11 1			T				
Command	APDU	APDU 80 A1 [IDID] [PRID] LC 00 LE 20						
Specification	CDATA	None						
Specification	RESPONSE	[IDHASH] [SW (2 b	ytes)]					
Parameter	IDID	Init data ID 0: Default User PIN hash (32 bytes) 1: PUK (32 bytes) 2: SEMK (32 bytes) 3: Card ID (8 bytes) 4: OTPK (32 bytes) 5: SMK (32 bytes) 6: Pre-reg host description (64 bytes)						
	PRID	7: Pre-reg host OTP key (32 bytes) Pre-reg host ID (0 ~ 6) Only used for IDID 6 and 7						
	IDHASH	SHA256 value of Init data (32 bytes)						
Note	None							

4.2.3. se_init_confirm

Command	se_init_conf	se_init_confirm						
Description	Confirm init	Confirm init data						
Supported	ISO, SPI	SO CDI						
Interfaces	130, 311							
Supported	00h. INIT	201 DUT						
Modes	OUII. IINI I	00h: INIT						
	APDU	80 A2 00 00	LC	00	LE	00		
Command	CDATA	None						
Specification	RESPONSE	None [SW (2 bytes)]						
Parameter	None							
	1. All init of	data should be set b	oeform	calling	this			
NT-4-	command							
Note	2. SE will transist to PERSO state after init data							
	confirme	ed						

4.2.4. se_init_vmk_chlng

Command	se_init_vmk	_chlng					
Description	Get VMK ch	Get VMK challenge					
Supported	ICO CDI	SO SDI					
Interfaces	130, 311	ISO, SPI					
Supported	00h: INIT						
Supported Modes	06h: NOHOST						
Wiodes	07h: DISCONN						
Command	APDU	80 A3 00 00	LC	00	LE	10	
0 0 22222022	CDATA	None					
Specification	RESPONSE [CHLNG] [SW (2 bytes)]						
Parameter	CHLNG	Auth challenge (16 bytes)					
Note	None						

4.2.5. se_init_back_init

Command	se_init_back	e_init_back_init						
Description	Back to INIT	Back to INIT state						
Supported	ISO, SPI	O SDI						
Interfaces	150, 511	50, 881						
Supported	06h: NOHOS	ST						
Modes	07h: DISCO	NN						
Command	APDU	80 A4 00 00	LC	10	LE	00		
Command	CDATA	[VMKRESP]						
Specification	RESPONSE	[SW (2 bytes)]						
Parameter	VMKRESP	VMK response (1	6 byte	es)				
	1. VMKRES	SP is calculated by						
	AES_EN	$C_{VMK}(CHLNG)$						
Note	2. CHLNG (challenge) is got from se_init_vmk_chlng							
Note	command							
	3. VMK aut	hentication should	be pa	ssed to b	ack IN	IIT		
	state succ	essfully						

4.2.6. se_init_change_vmk

Command	se_init_change_	_vmk					
Description	Change VMK						
Supported	ICO CDI						
Interfaces	ISO, SPI						
Supported	01h: INIT	O1h: INIT					
Modes	OIII. IINI I						
Command	APDU	80 A5 00 00	LC	50	LE	00	
Specification	CDATA	[VMKRESP] [WRPVMK] [HASH]				H]	
	RESPONSE	[SW (2 bytes)]					
	VMKRESP	VMK respons	se (16	bytes)			
Parameter	WRPVMK	Wrapped VMK (32 bytes)					
	HASH	SHA256 of W	/RPVI	MK (32	bytes)	s)	
	VMKRESF	is calculated b	Эy				
	AES_ENC	_{VMK} (CHLNG)					
NI a 4 a	• CHLNG (c	hallenge) is go	t from	se_init_	vmk_o	chlng	
Note	command						
	New VMK	is wrapped by	"old V	VMK"			
	• Encryption	algorithm is A	ES-25	6 ECB r	node		

4.3. Host Binding

4.3.1. se_bind_reg_init

Command	se_bind_reg_ii	nit				
Description	Init binding reg					
Supported Interfaces	ISO, SPI					
Supported	06h: NOHOST	O6h: NOHOST				
Modes	07h: DISCONN					
Command	APDU	80 D0 [FIRST] 00 LC 80 LE 0A				
	CDATA	[HSTCRED] [HSTDESC] [HASH]				
Specification	RESPONSE	[BRHANDLE] [OTP] [SW (2 bytes)]				
	FIRST	First registered host flag (1 byte)				
	HSTCRED	Host credential (32 bytes)				
	HSTDESC	Host description (64 bytes)				
Parameter	HASH	HASH of HSTCRED HSTDESC				
Parameter	пазн	(32 bytes)				
	BRHANDLE	Binding registration handle (4 bytes)				
	OTD	Composition of OTP key (6 bytes,				
	OTP	ASCII format)				
	FIRST is for in	ndicating this is the first registered host of				
Note	BCSE. It should	ld be set in the NOHOST mode and				
	cleared in the I	DISCONN mode.				

4.3.2. se_bind_reg_chlng

Command	se_bind_reg_chl	se_bind_reg_chlng					
Description	Get registration	challenge					
Supported	ISO SDI	SO, SPI					
Interfaces	150, 511						
Supported	06h: NOHOST						
Modes	07h: DISCONN						
G 1	APDU	80 D1 00 00	LC	04	LE	10	
Command	CDATA	[BRHANDLE]					
Specification	RESPONSE	[REGCHLNG] [SW (2 bytes)]					
Parameter	BRHANDLE	Binding registr	ation l	nandle (4	4 byte	es)	
Parameter	REGCHLNG	Registration challenge (16 bytes)					
Note	None						

4.3.3. se_bind_reg_finish

Command	se_bind_reg_fin	e_bind_reg_finish						
Description	Finish binding re	egistration						
Supported	ICO CDI							
Interfaces	ISO, SPI							
Supported	06h: NOHOST							
Modes	07h: DISCONN							
	APDU	80 D2 00 00	LC	24	LE	02		
Command	CDATA	[BRHANDLE] [F	REGRE	SP] [PIN	RESP]	ı		
Specification	RESPONSE	[HST_ID] [CO	NFIR	M] [SW	(2			
		bytes)]						
	BRHANDLE	Binding registration handle (4 bytes)						
-	REGRESP	Registration response (16 bytes)						
	PINRESP	PIN response (16 bytes)						
Parameter	PINKESP	Irrelevant for the "add host" case						
Farameter	HST_ID	Host ID (1 byte)						
		Confirmation status (1 byte)						
	CONFIRM	00h: Confirmed						
		01h: Not confirmed						
	PINCHLNO	G should be got f	rom se	e_pin_cl	nlng			
	command							
	PINRESP is	only necessary	for "re	egister 1	st host	"		
Note	case (FIRS)	flag is set in the	e se_b	ind_reg_	_init			
	command)							
	REGRESP =	= AES256(DevK	Key, Rl	EGCHL	NG),			
	where DevKey = SHA256(HSTCRED \parallel OTP)							

4.3.4. se_bind_reg_info

Command	se_bind_reg_i	nfo				
Description	Get registered	host info				
Supported Interfaces	ISO, SPI					
Supported Modes	01h: PERSO 02h: NORMA 03h: AUTH 04h: LOCK 06h: NOHOST 07h: DISCON	Γ				
	APDU	80 D3 [HST_ID] 00 LC 00 LE 81				
Command	CDATA	None				
Specification	RESPONSE	[BINDSTATE] [HSTDESC] [SW (2 bytes)]				
	HST_ID	Host ID (1 byte)				
Parameter	BINDSTATE	Binding status (1 byte) 00h: Empty 01h: Registered 02h: Confirmed				
	HSTDESC	Host description (64 bytes)				
Note	None					

4.3.5. se_bind_reg_approve

Command	se_bind_reg	se_bind_reg_approve					
Description	Approve und	Approve unconfirmed registered host					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported Modes		01h: PERSO 02h: NORMAL 03h: AUTH					
Command	APDU	80 D4 [HST_ID] 00	LC	00	LE	00	
0 0 111110110	CDATA	None					
Specification	RESPONSE [SW (2 bytes)]						
Parameter	HST_ID	Host ID (1 byte)					
Note	None						

4.3.6. se_bind_reg_remove

Command	se_bind_reg	se_bind_reg_remove					
Description	Remove reg	istered host					
Supported Interfaces	ISO, SPI	SO, SPI					
Supported Modes	01h: PERSC 02h: NORM 03h: AUTH	th: NORMAL					
Command	APDU	80 D5 [HST_ID] 00	LC	00	LE	00	
Command	CDATA	None					
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	HST_ID	Host ID (1 byte)					
Note	None						

4.3.7. se_bind_login_chlng

Command	se_bind_login_	se_bind_login_chlng				
Description	Get login challe	Get login challenge				
Supported	ISO, SPI	SO SDI				
Interfaces	130, 311					
Supported	07h: DISCONN	07h: DISCONN				
Modes	U/II. DISCONIV					
Command	APDU	80 D6 [HST_ID] 00	LC	00	LE	10
	CDATA	None				
Specification	RESPONSE	[BINDCHLNG] [S	W (2	bytes	3)]	
Parameter	HST_ID	Host ID (1 byte)				
Parameter	BINDCHLNG	Binding login chall	enge	(16 b)	ytes)	
Note	None					

4.3.8. se_bind_login

Command	se_bind_login						
Description	Host binding lo	lost binding login					
Supported	ICO CDI						
Interfaces	ISO, SPI						
Supported	07h. DISCONN	7h: DISCONN					
Modes	07h: DISCONN	n: DISCONN					
Command	APDU	80 D7 [HST_ID] 00 LC 10 LE 00					
	CDATA	[BINDRESP]					
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	HST_ID	Host ID (1 byte)					
Parameter	BINDRESP	Binding login response (16 bytes)					
	• After login	, the binding session (2 keys) is					
	established	. The established session keys are					
	denoted by	BIND_SENCK (Encryption key) and					
NI-4-	BIND_SM	ACK (MAC key)					
Note	• BIND_SEN	NCK = SHA256 (BINDCHLNG					
	OTPKEY	BINDRESP "ENC")					
	BIND SMACK = SHA256 (BINDCHLNG						
	OTPKEY	BINDRESP "MAC")					

4.3.9. se_bind_logout

Command	se_bind_logout	se_bind_logout					
Description	Host binding lo	Host binding logout					
Supported	ICO CDI						
Interfaces	150, 511	SO, SPI					
Cupported	01h: PERSO						
Supported Modes	02h: NORMAL						
Modes	04h: LOCK						
Command	APDU	80 D8 00 00	LC	00	LE	00	
0 0 11111011101	CDATA	None					
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	None						
Note	None						

4.3.10. se_bind_find_hstid

Command	se_bind_find_h	nst_id				
Description	Find registered	host ID by host cr	redent	ial		
Supported Interfaces	ISO, SPI	SO, SPI				
Supported Modes	01h: PERSO 02h: NORMAI 03h: AUTH 04h: LOCK 06h: NOHOST 07h: DISCONN					
	APDU 80 D9 00 00 LC 20					02
Command Specification	CDATA RESPONSE	[HSTCRED]			(2 byt	
	HSTCRED	Host credential (/1
Donomoton	HST_ID	Host ID (1 byte) HST_ID is FFh mea	<u> </u>	•	l host	
Parameter	CONFIRM	Confirmation status (1 byte) 00h: Confirmed 01h: Not confirmed				
Note	None					

4.3.11. se_bind_back_nohost

Command	se_bind_back_1	nohost					
Description	Back to NOHO	Back to NOHOST mode					
Supported	ICO CDI						
Interfaces	ISO, SPI						
Supported	01h: PERSO	01h: PERSO					
Modes	07h: DISCONN	1					
Command	APDU	80 DA 00 00	LC	30	LE	00	
	CDATA	[PINRESP] [PIN	HASF	H]			
Specification	RESPONSE	[SW (2 bytes)]					
	PINRESP	PIN response (16 bytes)					
Parameter -	FINKESP	For DISCONN mode only					
	PINHASH	New PIN hash (3)	2 byte	es)			
	FINIIASII	For PERSO mode only					
	• All wallet	data and perso data	will l	be clea	red		
	• PINCHLN	G should be got from	om se	_pin_c	hlng		
	command						
	PINRESP i	s only necessary for	or "ba	cking f	rom		
Note	DISCONN	mode" case. If ba	cking	from P	ERSC)	
Note	mode, just	set PINRESP as ze	ero.				
	• PINHASH	is encrypted by B	IND_S	SENC	X if		
	backing fro	om PERSO mode;	it's no	t neces	sary i	f	
	backing from DISCONN mode, just set PINHASH					SH	
	as zero.						

4.4.Personalization

4.4.1. se_perso_set_data

Command	se_perso_set	se_perso_set_data					
Description	Set perso da	ta					
Supported	ICO CDI						
Interfaces	ISO, SPI	SO, SPI					
Supported	01h: PERSO						
Modes	UIN. PERSO						
Command	APDU	80 30 [PDID] 00	LC	var.	LE	00	
	CDATA	[PERDATA] [PDMAC]					
Specification	RESPONSE	[SW (2 bytes)]					
	PDID	Perso data ID					
	מוטץ	0: Security policy (4	bytes)			
Parameter	PERDATA	Perso data (variable	length	1)			
	PDMAC	MAC of PERDATA	(32 by	rtes)			
	PDMAC	MAC key is BIND_S	SMA(CK			
Note	None						

4.4.2. se_perso_get_data_hash

Command	se_perso_ge	se_perso_get_data_hash					
Description	Get perso da	Get perso data hash					
Supported	ISO, SPI	SO SPI					
Interfaces	130, 311	SO, SPI					
Supported	01h: PERSO	•					
Modes	UIII. PERSO	Jin: PERSO					
Command	APDU	80 31 [PDID] 00	LC	00	LE	20	
	CDATA	None					
Specification	RESPONSE	[PDHASH] [SW (2	2 bytes)]			
	PDID	Perso data ID					
Parameter	מועץ	0: Security policy (4 byte	s)			
	PDHASH	SHA256 value of Perso data (32 bytes)					
Note	None						

4.4.3. se_perso_confirm

Command	se_perso_co	nfirm					
Description	Confirm per	Confirm perso data					
Supported	ISO, SPI	O SDI					
Interfaces	150, 511						
Supported	01h: PERSO	•					
Modes	UIII. FERSO	III. PERSO					
Command	APDU	80 32 00 00	LC	00	LE	00	
0 0 1 1 1 1 1 1 1	CDATA	None					
Specification	RESPONSE	None [SW (2 byte	es)]				
Parameter	None						
	1. All perso	data should be set	before	calling			
Note	se_perso_confirm						
Note	2. SE state will transist to NORMAL after perso data						
	confirme	d					

4.4.4. se_perso_back_perso

Command	se_perso_ba	se_perso_back_perso					
Description	Back to PER	SO state					
Supported	ICO CDI	SO, SPI					
Interfaces	130, 311						
Supported	02h: NORM	02h: NORMAL					
Modes	04h: LOCK	04h: LOCK					
Command	APDU	80 33 00 00	LC	20	LE	00	
	CDATA	[PINHASH]					
Specification	RESPONSE	[SW (2 bytes)]]				
Parameter	PINHASH	New PIN hash (32 bytes)					
Parameter	ПППАЗП	PINHASH is 6	encrypte	ed by B	IND_SI	ENCK	
Note	None						

4.5. Authentication

4.5.1. se_pin_chlng

Command	se_pin_chlng					
Description	Get PIN auth	challenge				
Supported	ICO CDI					
Interfaces	ISO, SPI	0, 511				
Cummonted	02h: NORMA	AL				
Supported Modes	06h: NOHOS	06h: NOHOST				
Modes	07h: DISCONN					
Command	APDU	80 20 00 00	LC	00	LE	10
	CDATA	None				
Specification	RESPONSE	[PINCHLNG]] [SW ((2 bytes)]	
Parameter	PINCHLNG	PIN challenge	e (16 by	ytes)		
	PINCHLNG (can be used for	PIN a	uthentic	ation	
Note	(se_pin_auth)	, first host regi	stration	1		
Note	(se_bind_reg_finish) and backing to NOHOST mode					
	from DISCO	NN mode (se_b	oind_ba	ack_noh	ost)	

4.5.2. se_pin_auth

Command	se_pin_auth	se_pin_auth					
Description	PIN authenti	cation					
Supported	ISO, SPI						
Interfaces	130, 311	SO, SPI					
Supported	02h NODM	ΑΙ					
Modes	UZII. INOKIVI	2h: NORMAL					
Command	APDU	80 21 00 00	LC	10	LE	00	
<u> </u>	CDATA	[PINRESP]					
Specification	RESPONSE	[SW (2 bytes)]]				
Parameter	PINRESP	PIN response	(16 byte	es)			
	• This cor	nmand can only	be exe	cuted s	uccessfi	ılly	
Note	when PI	N function is en	nabled in	n secur	ity polic	cy	
Note	• If auth passed, SE will enter AUTH mode						
	• RESP is	calculated by A	AES_EN	IC _{PINHA}	SH(CHL	NG)	

4.5.3. se_pin_change

Command	se_pin_change					
Description	Change PIN					
Supported	ISO, SPI					
Interfaces	130, 311					
Supported	03h: AUTH					
Modes	03II. AU 111	75H. 710 TT				
Command	APDU	80 22 00 00	LC	40	LE	00
Command Specification	CDATA	CDATA [WRPINHASH] [MAC]				
Specification	RESPONSE	[SW (2 bytes)]				
	WRPINHASH	Wrapped new	PIN ha	ash (32	bytes)	
Parameter	MAC	MAC of WRP	INHA:	SH (32	bytes))
	IVIAC	MAC key is BIND_SMACK				
Note	New PIN hash is wrapped by "old PIN hash"					
Note	• Encryption	algorithm is AE	ES-256	ECB r	node	

4.5.4. se_pin_logout

Command	se_pin_logo	ut				
Description	PIN logout					
Supported	ISO, SPI					
Interfaces	150, 511					
Supported	02h: NORMAL					
Modes	03h: AUTH					
Command	APDU	80 23 00 00	LC	00	LE	00
	CDATA	None				
Specification	RESPONSE	[SW (2 bytes)]]			
Parameter	None					
	• This cor	nmand can only	be exe	cuted s	uccessfi	ılly
Note	when PIN function is enabled in security policy					
	• After thi	is command SE	will en	ter UN	AUTH 1	node

4.5.5. se_puk_chlng

Command	se_puk_chln	se_puk_chlng					
Description	Get PUK ver	Get PUK verify challenge					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported Modes	04h: LOCK	04h: LOCK					
Command	APDU	80 24 00 00	LC	00	LE	10	
Command	CDATA	None					
Specification	RESPONSE	[CHLNG] [SV	V (2 byt	es)]			
Parameter	CHLNG	PUK auth chai	llenge (16 byte	s)		
Note		nd can only be CK functions ar			-		

4.5.6. se_pin_unlock

Command	se_pin_unlo	ck						
Description	Unlock PIN	Unlock PIN by PUK						
Supported	ICO CDI							
Interfaces	ISO, SPI							
Supported	Mh. I OCK	04h: LOCK						
Modes	04n. LOCK							
Command	APDU	80 25 00 00	LC	30	LE	00		
	CDATA	[RESP] [PINH	[ASH]					
Specification	RESPONSE	[SW (2 bytes)]						
	RESP	Verification re	sponse	(16 byt	es)			
Parameter	PINHASH	New PIN hash	(32 by	tes)				
	PINHASH	PINHASH is 6	encrypte	ed by B	IND_S	ENCK		
	• This cor	nmand can only	be exe	cuted s	uccessfi	ully		
	when PI	N and LOCK fo	unctions	s are en	abled in	ı		
Note	security	policy						
Note	• RESP is	calculated by A	AES_EN	VC _{PUK} (0	CHLNG	i)		
	CHLNG (challenge) is got from se puk chlng							
	comman	nd			·			

4.6.BCDC Setting

4.6.1. se_set_currency

Command	se_set_curre	ncy					
Description	Set currency	Set currency setting					
Supported	ICO CDI						
Interfaces	ISO, SPI						
	02h: NORM	AL					
Supported	03h: AUTH						
Modes	06h: NOHO	06h: NOHOST					
	07h: DISCONN						
	APDU	LE	00				
Command		[CURNCY]					
	CDATA	● BYTE[0]:	CurrTy	pe			
Specification		● BYTE[1 ~	~ 4]: Cu	rrRate,	big-end	lian	
	RESPONSE	[SW (2 bytes)]]				
Parameter	CURNCY	Currency setting	ng (5 by	rtes)			
Note	This command can be executed successfully only if SE						
Note	is persoed						

4.6.2. se_get_currency

Command	se_get_curre	ency					
Description	Get currency	Get currency setting					
Supported	ICO CDI	CO CDI					
Interfaces	ISO, SPI						
	02h: NORM	AL					
Supported	03h: AUTH	O3h: AUTH					
Modes	06h: NOHOST						
	07h: DISCO	07h: DISCONN					
Command	APDU	80 41 00 00	LC	00	LE	05	
	CDATA	None					
Specification	RESPONSE	[CURNCY] [S	SW (2 b)	ytes)]			
		Currency setting	ng (5 by	rtes)			
Parameter	CURNCY	● BYTE[0]:	CurrTy	pe			
		● BYTE[1 ~	- 4]: Cu	rrRate,	big-end	lian	
Note	This command can be executed successfully only if SE						
Note	is persoed						

4.6.3. se_get_card_name

Command	se_get_card_	_name					
Description	Get SE card	Get SE card name					
Supported	ICO CDI	ICO CDI					
Interfaces	130, 311	ISO, SPI					
	02h: NORM	AL					
Supported	03h: AUTH	3h: AUTH					
Modes	06h: NOHOST						
	07h: DISCO	NN					
C1	APDU	80 42 00 00	LC	00	LE	20	
Command	CDATA	None					
Specification	RESPONSE	[CARDNAMI	E] [SW	(2 bytes	s)]		
Parameter	CARDNAME	Card name (32	2 bytes)				
Note	This command can be executed successfully only if SE						
Note	is persoed						

4.6.4. se_set_card_name

Command	se_set_card_	name					
Description	Set SE card	Set SE card name					
Supported	ICO CDI						
Interfaces	ISO, SPI	50, SP1					
	02h: NORM	AL					
Supported	03h: AUTH	O3h: AUTH					
Modes	06h: NOHOST						
	07h: DISCO	NN					
C 1	APDU	80 43 00 00	LC	20	LE	00	
Command	CDATA	[CARDNAMI	Ξ]				
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	CARDNAME	Card name (32	bytes)				
Nata	This command can be executed successfully only if SE						
Note	is persoed						

4.6.5. se_get_secpo

Command	se get secpo							
Description		Get security policy setting						
Supported Interfaces	ISO, SPI							
Supported Modes	03h: AUTH 06h: NOHO 07h: DISCO	06h: NOHOST 07h: DISCONN						
Command	APDU	80 44 00 00	LC	00	LE	04		
Specification	CDATA	None						
Specification	RESPONSE	[SECPO] [SW	(2 byte	es)]				
Parameter	SECPO	Security policy ■ BYTE[0]: ■ BIT[0]: verifice ■ BIT[1]: ■ BIT[2]: ■ BIT[3]: ■ BIT[4]: ■ BIT[5]: ■ BIT[6 ~ ■ BYTE[1 ~	Trx signation Trx signation PIN vention PIN LO Watchl Display	gning O gning bu crification OCK m Dog ena	TP utton co on echanis able			
Note	None							

4.6.6. se_set_secpo

Command	se set secpo)						
Description		Set security policy setting						
Supported Interfaces	ISO, SPI	ISO, SPI						
	02h: NORM	AL						
Supported	03h: AUTH							
Modes	06h: NOHO	ST						
	07h: DISCO	NN						
C1	APDU	80 45 00 00	LC	04	LE	00		
Command	CDATA	[SECPO]						
Specification	RESPONSE	ONSE [SW (2 bytes)]						
		Security policy setting (4 bytes)						
		● BYTE[0]:						
		■ BIT[0]:	Trx sig	ning O	TP			
		verific	cation					
		■ BIT[1]:	Trx sig	ning bu	ıtton co	nfirm		
Parameter	SECPO	■ BIT[2]:	PIN ve	rification	on			
		■ BIT[3]:	PIN LO	OCK m	echanis	m		
		■ BIT[4]: WatchDog enable						
		■ BIT[5]: Display Address						
	■ BIT[6 ~ 7]: rfu							
	● BYTE[1 ~ 3]: rfu							
Note	None							

4.6.7. se_get_card_id

Command	se_get_card_	_id						
Description	Get SE card	Get SE card ID						
Supported Interfaces	ISO, SPI	ISO, SPI						
Supported Modes	03h: AUTH	06h: NOHOST						
	APDU	80 46 00 00	LC	00	LE	08		
Command	CDATA	None						
Specification	RESPONSE	[CARDID] [S	W (2 by	rtes)]				
Parameter	CARDID	Card ID (8 bytes)						
Note	None							

4.7.Transaction Signing

4.7.1. se_trx_status

Command	se_trx_status	se_trx_status					
Description	Get transacti	Get transaction signing status					
Supported	ICO CDI	IGO, GDI					
Interfaces	ISO, SPI	150, 511					
Supported	02h: NORM	02h: NORMAL					
Modes	03h: AUTH						
Command	APDU	80 80 00 00	LC	00	LE	01	
Command	CDATA	None					
Specification	RESPONSE	[TRXSTAT] [SW (2 bytes)]					
		Transaction signing status (1 byte)					
		00h: Idle					
Parameter	TRXSTAT	01h: Transaction signing in preparing					
Parameter	IKASIAI	02h: Transaction signing beginned					
		03h: Transaction signing OTP verified					
		04h: Transaction signing in progress					
Note	If PIN function is enabled, this command can only be						
Note	executed suc	cessfully in AUTH	I mode				

4.7.2. se_trx_begin

Command	se_trx_begin					
Description	Transaction s	signing begins				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORM	AL				
Modes	03h: AUTH					
Command	APDU	APDU 80 72 00 00 LC 38 LE 06				06
Command	CDATA	CDATA [AMOUNT] [ENCOUTADDR]				
Specification	RESPONSE	[OTP] [SW (2 byte	es)]			
	AMOUNT	Transaction amou	nt (8 b	ytes, big	g-endi	an)
Parameter	ENCOUTADDR	Encrypted output a	addres	s (48 by	tes)	
Parameter	ENCOUTADDR	The encryption ke	y is Bl	ND_SE	NCK	
	OTP	OTP digits (6 byte	s, ASC	CII form	at)	
	If PIN function is enabled, this command can only					
Note	be execu	ted successfully in	AUTH	mode		
Note	• If OTP for	unction is disabled,	the ou	tput OT	P is a	11
	zero					

4.7.3. se_trx_verify_otp

Command	se_trx_verify	y_otp				
Description	Verify OTP	Verify OTP				
Supported	ISO, SPI					
Interfaces	150, 511					
Supported	02h: NORM	AL				
Modes	03h: AUTH	03h: AUTH				
Command	APDU	80 73 00 00	LC	06	LE	00
0 0 22222022 02	CDATA	[OTP]				
Specification	RESPONSE	[SW (2 bytes)]				
Parameter	OTP	OTP digits (6 byte	es)			
	• If PIN fo	unction is enabled,	this co	mmand	can oi	nly
Note	be executed successfully in AUTH mode					
Note	• If OTP f	If OTP function is disabled, any OTP value can				
	pass ver	ification				

4.7.4. se_trx_sign

Command	se_trx_sign					
Description	Sign transact	tion				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORM	AL				
Modes	03h: AUTH					
Command	APDU	APDU 80 74 [IN_ID] 00 LC 00 LE 60				60
Command	CDATA	CDATA None				
Specification	RESPONSE	[SIG] [SIGMAC][S	SW (2	bytes)]		
	IN_ID	Input ID (1 byte, 0	~ 255)		
Parameter	SIG	Signature (64 bytes)			
Parameter	SIGMAC	MAC of signature ((32 by	tes)		
	SIGNIAC	MAC Key is BIND	_SMA	ACK		
	• If PIN fo	• If PIN function is enabled, this command can only				
Note	be execu	ited successfully in A	AUTH	l mode		
Note	 Signature material is set in se_trx_prepare 					
	• Input ID	must be those set in	se_tr	x_prepa	re	

4.7.5. se_trx_get_ctxinfo

Command	se_trx_get_c	etxinfo					
Description	Get transacti	on signing context info					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported	02h: NORM	AL					
Modes	03h: AUTH						
	APDU	80 75 [IN_ID] 00 LC 00 LE 2E					
Command	CDATA	None					
Specification Specification	RESPONSE	[NUMIN] [SITYP] [WAID] [ACCID] [KCID] [KEYID] [SIGMTRL] [SW (2 bytes)]					
	IN_ID	Input ID (1 byte, 0 ~ 255)					
	NUMIN	Number of inputs (2 bytes, little-endian)					
	SITYP	Signing type (1 byte) 00h: HDW 01h: XCHS (Exchange site) 02h: Old-wallet					
Parameter	WAID	Signing wallet ID (2 bytes, little-endian) Only effective in Old-wallet type					
	ACCID	Signing account ID (4 bytes, little-endian) Only effective in HDW or XCHS type					
	KCID	Key chain ID (1 byte) Only effective in HDW or XCHS type					
_	KEYID	Key ID (4 bytes, little-endian) Only effective in HDW or XCHS type					
	SIGMTRL	ATRL Signature material (32 bytes)					
Note		unction is enabled, this command can only uted successfully in AUTH mode					

4.7.6. se_trx_finish

Command	se_trx_finish	1				
Description	Finish transa	ection signing				
Supported	ISO, SPI					
Interfaces	150, 51 1					
Supported	02h: NORM	AL				
Modes	03h: AUTH	03h: AUTH				
Command	APDU	80 76 00 00	LC	00	LE	00
0 0 1111111111	CDATA	None				
Specification	RESPONSE	[SW (2 bytes)]				
Parameter	None					
	• If PIN fo	unction is enabled,	this co	mmand o	can or	nly
Note	be executed successfully in AUTH mode					
Note	Signing	Signing status is set to be IDLE				
	• All cont	ext info are cleared	1			

4.7.7. se_trx_outaddr

Command	se_trx_outad	dr				
Description	Get trx signin	ng output address				
Supported	SPI					
Interfaces	SPI					
Supported	02h: NORM	AL				
Modes	03h: AUTH					
C1	APDU	APDU 80 79 00 00 LC 00 LE 22				22
Command	CDATA	None				
Specification	RESPONSE	[OUTADDR] [SV	W (2 by	tes)]		
Parameter	OUTADDR	Output address (3	34 bytes	s)		
Parameter	None					
	• If PIN fu	inction is enabled,	this cor	nmand	can oi	nly
	be execu	ted successfully in	a AUTH	I mode		
Note	• Signing	• Signing status must be in BEGIN or VERIFIED)
	This output address is only used in HDW signing				ıg	
	type, oth	er type will just ou	ıtput ze	ros		

4.9.HD Wallet

4.9.1. se_hdw_init_wallet

Command	se_hdw_init_w	vallet				
Description	Initialize HDW	Initialize HDW				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORMA	L				
Modes	03h: AUTH					
Command	APDU	80 B0 00 00	LC	80	LE	00
	CDATA	CDATA [HDWNAME] [EMKSEED] [MAC]				
Specification	RESPONSE	RESPONSE [SW (2 bytes)]				
	HDWNAME	HD wallet name (32 byt	es)		
	EMKSEED	Encrypted HDW 1	naster	key see	ed (64	
Parameter	EWINSEED	bytes)				
	MAC	MAC value of EM	IKSEI	ED		
	IVIAC	MAC key is BINI	D_SM	ACK		
	• If PIN function is enabled, this command can only be				y be	
Note	executed s	uccessfully in AUT	TH mo	de		
Note	• HDW mus	st be in INACTIVE	state			
	• EMKSEE	D is encrypted by E	BIND_	SENCK		

4.9.2. se_hdw_init_wallet_gen

Command	se_hdw_init_wa	llet_gen				
Description	Initialize HDW	Initialize HDW (gen key)				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORMAL					
Modes	03h: AUTH					
	APDU	APDU 80 B1 00 00 LC var. LE				var.
Command	CDATA	[HDWNAME] [PASSPHR]	[NUL	EN] [PA	ALEN	[]
Specification	[NUMSET] [ACTVC		RESPONSE [NUMSET] [ACTVCOD			
	RESI ONSE	[SW (2 bytes)]				
	HDWNAME	HD wallet name (32 bytes)				
	NULEN	Number set length (1 byte, 24, 36 or				
	NOLLIV	48)				
	PALEN	Pass phrase len	igth (1	byte, 0	~ 16)	
Parameter	PASSPHR	Pass phrase (va	ar. leng	th)		
	NUMSET	Number set (va	ar. leng	th, BCI) forn	nat)
	ACTVCODE	Activation cod	e (4 by	tes)		
	MAC	MAC of NUM	SET .	ACTVO	CODE	E
	MAC key is BIND_SMACK					
	If PIN function is enabled, this command can			can o	nly	
Note	be executed	successfully in	AUTH	mode		
	• HDW must	be in INACTIV	E state			

4.9.3. se_hdw_qry_wa_info

Command	se_hdw_qry_wa	ı_info	se_hdw_qry_wa_info				
Description	Query HDW inf	co co					
Supported Interfaces	ISO, SPI						
Supported Modes	02h: NORMAL 03h: AUTH 06h: NOHOST 07h: DISCONN	03h: AUTH 06h: NOHOST					
Command	APDU	80 B2 [INFOID] 00	LC	00	LE	var.	
Specification	CDATA	None					
Specification	RESPONSE	[HDWINFO] [SW	/ (2 by	tes)]			
Parameter	INFOID	HDW info ID 00h: HDW status 01h: HDWname (1 02h: HDW accour 03h: All HDW inf	32 byt nt poin	es) ter (4	•	s)	
	HDWINFO	HDW info (variab	le leng	gth)			
Note	 HDW status: 00h: INACTIVE 01h: WAITACTV 02h: ACTIVE All HDW info: [HDW status] [HDWname] [HDW account pointer] (37 bytes) 						

4.9.4. se_hdw_set_wa_info

Command	se_hdw_set_wa	se_hdw_set_wa_info				
Description	Set HDW info					
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORMAL					
Modes	03h: AUTH					
Command	APDU	80 B3 [INFOID] 00	LC	var.	LE	00
	CDATA	CDATA [HDWINFO]				
Specification	RESPONSE	[SW (2 bytes)]				
		HDW info ID (32	bytes	s)		
Parameter	INFOID	01h: HDWname (32 by	rtes)		
Parameter		02h: HDW accoun	nt poi	nter (4	bytes	s)
	HDWINFO HDW info (variable length)					
Note	If PIN function is enabled, this command can only be			e		
Note	executed succes	sfully in AUTH mo	ode			

4.9.5. se_hdw_create_account

Command	se_hdw_create_	account				
Description	Create HDW acc	count				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORMAL					
Modes	03h: AUTH					
C1	APDU	APDU 80 B4 00 00 LC 24 LE 00				00
Command	CDATA	CDATA [ACCID] [ACCNAME]				
Specification	RESPONSE	[SW (2 bytes)]				
Danamatan	ACCID	Account ID (4 b	ytes, l	little-en	dian)	
Parameter	ACCNAME	Account name (32 by	tes)		
	• If PIN funct	tion is enabled, th	is con	nmand	can oi	nly
	be executed	successfully in A	UTH	mode		
Note	 Account ID must be equal to current account pointer 					
	Key pointer	s of the previous	accou	nt cann	ot be	0

4.9.6. se_hdw_qry_acc_info

Command	se_hdw_qry_	acc_info		
Description	Query HDW	account info		
Supported Interfaces	ISO, SPI	ISO, SPI		
	02h: NORM	AL		
Supported	03h: AUTH			
Modes	06h: NOHOS	ST		
	07h: DISCO	NN		
C1	APDU	80 B5 [INFOID] 00 LC 04 LE var.		
Command	CDATA	[ACCID]		
Specification	RESPONSE	[ACCINFO] [SW (2 bytes)]		
Parameter	INFOID	Account info ID (1 byte) 00h: Account name (32 bytes) 01h: Balance (8 bytes, big-endian) 02h: External key pointer (4 bytes, little-endian) 03h: Internal key pointer (4 bytes, little-endian) 04h: Exchange site blocked balance (8 bytes, big-endian) 05h: All account info (56 bytes)		
	ACCID	Account ID (4 bytes, little-endian)		
	ACCINFO	FO Output account info (variable length)		
	All account is	nfo (56 bytes):		
Note	[Account name] [Balance] [External key points [Internal key pointer] [Ex-site blocked balance]			

4.9.7. se_hdw_set_acc_info

Command	se hdw set	acc info				
Description	Set HDW acc	et HDW account info				
Supported	ISO, SPI	SO SPI				
Interfaces	150, 511	50, 51 1				
Supported	02h: NORM	AL				
Modes	03h: AUTH					
C1	APDU	80 B6 [INFOID] 00	LC	var.	LE	00
Command	CDATA	[ACCID] [ACCINF	O] [N	IAC]		
Specification	RESPONSE	[SW (2 bytes)]				
		Account info ID (1 byte)				
		00h: Account name (32 bytes)				
	INFOID	01h: Balance (8 bytes)				
		02h: External key po	ointer	(4 byte	es)	
Parameter		03h: Internal key po	inter	(4 byte	es)	
	ACCID	Account ID (4 bytes	, little	e-endia	ın)	
	ACCINFO	Output account info	(varia	able le	ngth)	
	MAC	MAC value for ACC	CINFO	O (32 b	ytes)	
	IVIAC	MAC key is BIND_	SMA	CK		
Note	If PIN function	on is enabled, this cor	nman	d can	only b	e
Note	executed succ	cessfully in AUTH m	ode			

4.9.8. se_hdw_next_trx_addr

Command	se_hdw_next	_trx_addr				
Description	Get next trx a	address				
Supported	ICO CDI					
Interfaces	ISO, SPI					
Supported	02h: NORMA	AL				
Modes	03h: AUTH					
Command	APDU	80 B7 [KCID] 00 LC 04 LE 3D				
Specification	CDATA	[ACCID]				
Specification	RESPONSE	[KID] [ADDR] [MAC] [SW (2 bytes)]				
		Key Chain ID (1 byte)				
	KCID	00h: External chain				
		01h: Internal chain				
Parameter	ACCID	Account ID (4 bytes, little-endian)				
Parameter	KID	Key ID (4 bytes, little-endian)				
	ADDR	Output trx address (25 bytes)				
	MAC	MAC value for (KID ADDR) (32 bytes)				
	IVIAC	MAC key is BIND_SMACK				
Note	If PIN function	on is enabled, this command can only be				
Note	executed succ	cessfully in AUTH mode				

4.9.9. se_hdw_prep_trx_sign

Command	se_hdw_prep	_trx_sign				
Description	Prepare HDV	Prepare HDW trx signing				
Supported Interfaces	ISO, SPI	SO, SPI				
Supported	02h: NORM	AL				
Modes	03h: AUTH	3h: AUTH				
Command	APDU	80 B8 [IN_ID] [KCID]	LC	50	LE	00
	CDATA	[ACCID] [KID] [BALN	IC] [SI	GMTRI	L] [MA	C]
Specification	RESPONSE	[SW (2 bytes)]				
	IN_ID	Input ID (1 byte, 0 ~	255)			
		Key Chain ID (1 byte)				
	KCID	00h: External chain				
		01h: Internal chain				
	ACCID	Account ID (4 bytes	, little-	-endia	1)	
Parameter	KID	Key ID (4 bytes, little-endian)				
Parameter	BALNC	Transaction amount	for thi	s inpu	t (8	
	DALNC	bytes)				
	SIGMTRL	Signature material (3	32 byte	es)		
		MAC value of signa	ture in	put da	ta	
	MAC	(ACCID KID BA	LNC	SIGI	MTRL)
		MAC key is BIND_	SMAC	CK		
	• If PIN fo	unction is enabled, thi	s com	mand	can on	ly
	be execu	ited successfully in A	UTH 1	node		
Note	• IN_ID h	as to start from 0, and	l must	be inp	ut in	
Note	serial					
	• Key (dec	cided by ACCID and	KID)	cannot	repeat	
	• BALAN	CE will be substracte	d fron	n this a	ccoun	t

4.9.10. se_hdw_init_wallet_gen_confirm

Command	se_hdw_init_wa	llet_gen_confiri	n				
Description	Confirm HDW i	Confirm HDW initialization (gen key)					
Supported	ICO CDI	CO SDI					
Interfaces	ISO, SPI						
Supported	02h: NORMAL						
Modes	03h: AUTH						
Command	APDU	80 B9 00 00	LC	0A	LE	00	
Command	CDATA	[ACTVCODE] [NUCHKSUM]					
Specification	RESPONSE	[SW (2 bytes)]					
	ACTVCODE	Activation cod	e (4 by	tes)			
Parameter	NUCHKSUM	Number set checksum (6 bytes, ASCII					
	NUCHKSUM	format)					
	If PIN funct	ion is enabled, t	his con	nmand	can or	nly	
	be executed	successfully in	AUTH	mode			
Note	ACTVCOD	E is got from se	_hdw_	init_wa	llet_g	en	
Note	• HDW must	be in INACTIV	E state				
	• NUCHKSU	M = Sum of Nu	mSet A	SCII S	tring	(6	
	digits)						

4.9.11. se_hdw_qry_acc_keyinfo

Command	se_hdw_qry	_acc_keyinfo				
Description	Query HDW	account key info				
Supported Interfaces	ISO, SPI	SO, SPI				
Supported	02h: NORM	[AL				
Modes	03h: AUTH					
Command	APDU	80 BA [KINFOID] [KCID]	LC	08	LE	var.
	CDATA	[ACCID] [KID]				
Specification	RESPONSE	[ACCINFO] [MAC] [S	SW (2	byte	es)]	
	KINFOID	Account key info ID (1 byte) 00h: Address (25 bytes) 01h: Public key (64 bytes) 02h: Key chain public key and chain code (96 bytes)				
	ACCID	Account ID (4 bytes, little-endian)				
Parameter	KCID	Key Chain ID (1 byte) 00h: External chain 01h: Internal chain				
	KID	Key ID (4 bytes, little-	endia	n)		
	ACCINFO	Output account info (va	ariabl	e len	gth)	
	MAC	MAC value of ACCIN	`	•	tes)	
Note	irrelevar ■ Key cha ■ Key	KINFOID 02h (Key chain public key), KII				

4.10. Mailbox

4.10.1. mbox_spi_get_msg

Command	mbox_spi_get_r	nbox_spi_get_msg					
Description	Get mailbox me	ssage					
Supported	CDI	PI					
Interfaces	SP1						
Supported	All mades aver	+ EDDOD					
Modes	All modes excep	I EKKOK					
Command - Specification -	APDU	80 E0 00 00	LC	00	LE	81	
	CDATA	None					
Specification	RESPONSE	[MSGLEN] [MSG] [SW (2 bytes)]					
Parameter	MSGLEN	Message length	ı (2 byt	es, little	e-endi	ian)	
Parameter	MSG	Message (1281	bytes)				
	After mailbe	ox message is go	ot from				
Note	mbox_spi_g	get_msg, the mai	ilbox w	ill be e	mpty		
Note	Message is of fixed length, effective length is						
	indicated by	MSGLEN					

4.10.2. mbox_spi_send_resp

Command	mbox_spi_send_	mbox_spi_send_resp				
Description	Send response to	Send response to mailbox				
Supported	SPI	Dī				
Interfaces	561					
Supported	All modes execu	st EDD∩D				
Modes	All modes excep	All modes except ERROR				
Command	APDU	80 E1 00 00	LC	var.	LE	00
	CDATA	None				
Specification	RESPONSE	[RESP] [SW (2	2 bytes))]		
Parameter	RESP	Response (1 ~	128 by	tes)		
	The sent respons	se will be stored	in the	buffer o	of SE,	it
NI a 4 a	will stay in the b	ouffer until it is i	eceive	d by the	othe	r
Note	entity via ISO7816 interface, or replaced by newly sent					
	response					

4.10.3. mbox_iso_send_msg

Command	mbox_iso_send	nbox_iso_send_msg					
Description	Send mailbox m	end mailbox message					
Supported	ISO	O					
Interfaces	150						
Supported	All modes avec	All modes except ERROR					
Modes	An modes excep						
Command	APDU	80 E8 00 00	LC	var.	LE	00	
	CDATA	[MSG]					
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	MSG	Message (1 ~ 1	28 byte	es)			
Note	The message car	n be read by mb	ox_spi	_get_m	sg via	SPI	
Note	interface						

4.10.4. mbox_iso_get_resp

Command	mbox_iso_get_r	mbox_iso_get_resp					
Description	Get response to	Get response to mailbox					
Supported	ISO	O					
Interfaces	150						
Supported	All modes excer	1 modes execut EDDOD					
Modes	An modes excep	All modes except ERROR					
Command	APDU	80 E9 00 00	LC	00	LE	81	
	CDATA	None					
Specification	RESPONSE	[RESPLEN] [F	RESP][SW (2	bytes))]	
Parameter	RESPLEN	Response lengt	th (2 by	tes, littl	e-end	lian)	
Parameter	RESP	Response (128	bytes)				
Nada	Response is of f	ixed length 128	bytes, t	he effe	ctive		
Note	length is indicated by RESPLEN						

4.11. Exchange Site

4.11.1. se_xchs_reg_status

Command	se_xchs_reg_s	se_xchs_reg_status					
Description	Get registration	n status					
Supported	ICO CDI	O. C.D.					
Interfaces	ISO, SPI						
	02h: NORMA	th: NORMAL					
Supported	03h: AUTH	Bh: AUTH					
Modes	06h: NOHOST						
	07h: DISCON	07h: DISCONN					
Command	APDU	80 F0 00 00	LC	00	LE	01	
0 0 1111111111	CDATA	None					
Specification	RESPONSE	[REGSTAT] [SW	(2 byte	es)]			
		Exchange site reg	istratic	n status	s (1 by	te)	
Parameter	REGSTAT	00h: NOT_REGIS	STERE	ED			
Parameter	REGSIAI	01h: REG_INIT					
		02h: REGISTERE	ED_				
Note	None						

4.11.2. se_xchs_reg_init

Command	se_xchs_reg_ii	nit					
Description	Registration in	it					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported	02h: NORMA	02h: NORMAL					
Modes	03h: AUTH	O3h: AUTH					
C1	APDU	APDU 80 F1 [QRY] 00 LC 20 LE 30				30	
Command	CDATA	[USREMAIL]					
Specification	RESPONSE	[NONCE] [MAC]	[SW	(2 bytes	3)]		
Parameter	QRY	Query flag (1 byte If query flag is cleared generated and MAC calculated. The regist NOT_REGISTERED If query flag is set (not registration state must MAC generated/calculated) directly instead of generated will be ignored.	value of val	of user endestate muse value), the EG_INIT.	mail will st be he Nonce Il be ou	and tput	
	USREMAIL	User email (32 by	tes)				
	NONCE	Random material	for M	AC (16	bytes)		
	MAC	MAC value of (US) (32 bytes) MAC key is XCHS_S		IAIL N	NONC	E)	
Note		n is enabled, this co essfully in AUTH m		d can or	nly be		

4.11.3. se_xchs_reg_finish

Command	se_xchs_reg_f	inish					
Description	Registration fi	nish					
Supported Interfaces	ISO, SPI	SO, SPI					
Supported	02h: NORMA	L					
Modes	03h: AUTH						
Command	APDU	80 F2 00 00	LC	70	LE	30	
	CDATA	[EOTPK] [ESMK] [MAC] [NONCE]					
Specification	RESPONSE	[REGTKN] [NON	ICESE	[SW ((2 byte	es)]	
	ЕОТРК	Exchange site login OTP key (Encrypt by XCHS_SEMK, 32 bytes)					
	ESMK	Exchange site sess (Encrypted by XC			•	es)	
Parameter	MAC	MAC value of (EOTPK ESMK) (32 bytes) MAC key is XCHS_SEMK					
	NONCE	Nonce for REGTOKEN (16 bytes)					
	REGTKN	Registration token	(32 by	ytes)			
	NONCESE	Nonce for REGTOKEN generated by SE (16 bytes)					
	• If PIN fun	ction is enabled, thi	is com	mand c	an only	y be	
	executed s	successfully in AUT	TH mod	de			
	• REGTOK	EN is MAC value o	of the f	ollowir	ng data		
	(MAC key	is XCHS_SEMK)	:				
	■ CARI	D_ID					
Note	■ UID						
	■ UserE	Email					
	■ LOGI	N_OTPKEY					
	■ SESS	ION_MK					
	nonce	_Svr					
	nonce	_SE					

4.11.4. se_xchs_reg_clear

Command	se_xchs_reg_c	lear					
Description	Clear registrati	Clear registration status					
Supported	ISO, SPI	ICO CDI					
Interfaces	130, 311						
Supported	02h: NORMA	L					
Modes	03h: AUTH	03h: AUTH					
Command	APDU	80 F3 00 00	LC	00	LE	00	
0 0 22222022 02	CDATA	None					
Specification	RESPONSE	None					
Parameter	None						
	• If PIN function is enabled, this command can only be						
Note	executed s	uccessfully in AUT	TH mod	de			
Note	• The registr	ration status must b	e REG	INIT	or		
	REGISTE	RED					

4.11.5. se_xchs_get_otp

Command	se_xchs_get_o	tp						
Description	Get exchange	Get exchange site OTP						
Supported	ISO, SPI	SO SDI						
Interfaces	150, 511							
	02h: NORMA	2h: NORMAL						
Supported	03h: AUTH	O3h: AUTH						
Modes	06h: NOHOSา	06h: NOHOST						
	07h: DISCON	N						
Command	APDU	80 F4 00 00	LC	00	LE	06		
0 0 22222022	CDATA	None						
Specification	RESPONSE	[OTP] [SW (2 byt	es)]					
Parameter	OTP	Exchange site log	in OTI	digits	(6 byte	es)		
rarameter	OIP	ASCII format						
Note	The registratio	n status must be RI	EGIST	ERED				

4.11.6. se_xchs_session_init

Command	se_xchs_sessio	se_xchs_session_init					
Description	Exchange site	Exchange site session init					
Supported	ISO SDI	SO, SPI					
Interfaces	150, 511						
Supported	02h: NORMA	02h: NORMAL					
Modes	03h: AUTH	03h: AUTH					
C1	APDU	80 F5 00 00	LC	10	LE	20	
Command	CDATA	[SVRCHLNG]					
Specification	RESPONSE	[SERESP] [SECH	ILNG]	[SW (2	bytes)]	
	SVRCHLNG	Server challenge ((16 by	tes)			
Parameter	SERESP	SE response (16 b	ytes)				
	SECHLNG SE challenge (16 bytes)						
Note	The registratio	n status must be RI	EGIST	ERED			

4.11.7. se_xchs_session_estab

Command	se_xchs_sessio	on_estab						
Description	Exchange site	Exchange site session establish						
Supported	ISO, SPI	SO SDI						
Interfaces	150, 511							
Supported	02h: NORMA	L						
Modes	03h: AUTH	03h: AUTH						
Command	APDU	80 F6 00 00	LC	10	LE	00		
0 0 22222022 02	CDATA	[SVRRESP]						
Specification	RESPONSE	[SW (2 bytes)]						
Parameter	SVRRESP	Server response (1	6 byte	es)				
	• The registr	ration status must b	e REC	SISTER	ED			
Note	• The establ	ished session key is	scalle	d XCHS	S_SK,			
Note	which is S	HA256(SMK SV	R_CH	LNG				
	SE_CHLN	VG)						

4.11.8. se_xchs_session_logout

Command	se_xchs_session	se_xchs_session_logout					
Description	Logout established session						
Supported	ICO CDI	SO CDI					
Interfaces	130, 311	SO, SPI					
Supported	02h: NORMA	02h: NORMAL					
Modes	03h: AUTH	03h: AUTH					
Commond	APDU	80 F7 00 00	LC	00	LE	00	
Command	CDATA	None					
Specification	RESPONSE	[SW (2 bytes)]					
Parameter	None						
Note	The registration status must be REGISTERED						
Note	XCHS ses	sion status will be a	reset to	iDLE			

4.11.9. se_xchs_block_info

Command	se_xchs_bloc	se_xchs_block_info							
Description	Get blocking	info							
Supported	ISO SDI	CO CDI							
Interfaces	150, 511	SO, SPI							
Supported	02h: NORMA	AL							
Modes	03h: AUTH								
	APDU	80 F8 00 00	LC	04	LE	0D			
Command	CDATA	[OKTKN]							
Specification	RESPONSE	[STATE] [ACCID] [AMC	OUNT]					
		[SW (2 bytes)]							
	OKTKN	OK token (4 bytes)							
Parameter	STATE	Block info status (1	byte)						
Parameter	ACCID	Account ID (4 bytes	, little	e-endiar	n)				
	AMOUNT	Amount (8 bytes, big	g-end	ian)					
Note	• The regis	stration status must be	REC	SISTER	ED				
Note	• XCHS se	ession status must be e	establ	ished					

4.11.10. se_xchs_block_btc

Command	se_xchs_block	z_btc				
Description	Block account	Bitcoin				
Supported Interfaces	ISO, SPI					
Supported	02h: NORMA	L				
Modes	03h: AUTH	O3h: AUTH				
	APDU	80 F9 00 00 LC 40 LE 64				
Command	CDATA	[TRXID] [ACCID] [AMOUNT] [MAC1] [NONCE]				
Specification	RESPONSE	[BLKSIG] [OKTKN] [ENC_UBLKTKN] [MAC2] [NONCESE] [SW (2 bytes)]				
	TRXID	Transaction ID (4 bytes)				
	ACCID	Account ID (4 bytes, little-endian)				
	AMOUNT	Block amount (8 bytes, big-endian)				
	MAC1	MAC value of (TRXID ACCID AMOUNT) (32 bytes) MAC key is XCHS_SK				
	NONCE	Nonce for block signature (16 bytes)				
Parameter	BLKSIG	Block signature (32 bytes)				
	OKTKN	OK token (4 bytes)				
	ENC_UBLKTKN	Encrypted unblock token (16 bytes)				
	MAC2	MAC value of (BLKSIG OKTKN UBLKTKN) (32 bytes) MAC key is XCHS_SK				
	NONCESE	Nonce for block signature generated by SE (16 bytes)				
	• The regist	ration status must be REGISTERED				
	XCHS ses	sion must be established				
	BLKSIG i	s MAC value of the following data (MAC				
Note	key is XC	HS_SMK):				
	■ CARI	O_ID				
	■ UID					
	■ TRX_	ID				

- ACC
- AMOUNT
- nonce
- nonce_SE
- Unblock token (16 bytes) is composed of:
 - BYTE $[0 \sim 7]$: Prefix
 - BYTE $[8 \sim 15]$: Amount

4.11.11. se_xchs_cancel_block

Command	se_xchs_cance	el_block			
Description	Cancel Bitcoir	blocking			
Supported Interfaces	ISO, SPI				
Supported	02h: NORMA	L			
Modes	03h: AUTH				
	APDU	80 FA 00 00 LC 48 LE 50			
Command Specification	CDATA	[TRXID] [OKTKN] [ENC_UBLKTKN] [MAC1] [NONCE]			
	RESPONSE	[UBLKSIG] [MAC2] [NONCESE] [SW (2 bytes)]			
	TRXID	Transaction ID (4 bytes)			
	OKTKN	OK token (4 bytes)			
	ENC_UBLKTKN	Encrypted unblock token (16 bytes)			
Parameter -	MAC1	MAC value of (TRXID OKTKN UBLKTKN) (32 bytes) MAC key is XCHS_SK			
	NONCE	Nonce for unblock signature (16 bytes)			
	UBLKSIG	Unblock signature (32 bytes)			
	MAC2	MAC value of UBLKSIG (32 bytes) MAC key is XCHS_SK			
	NONCESE	Nonce for unblock signature generated by SE (16 bytes)			
Note	 XCHS ses UBLKSIC key is XC ■ CARI ■ UID ■ TRX_ ■ ACC 	 The registration status must be REGISTERED XCHS session must be established UBLKSIG is MAC value of the following data (MAC key is XCHS_SMK): CARD_ID UID TRX_ID ACC AMOUNT 			

- nonce_SE
- Unblock token (16 bytes) is composed of:
 - BYTE $[0 \sim 7]$: Prefix
 - BYTE [8 ~ 15]: Amount

4.11.12. se_xchs_trxsign_login

Command	se_xchs_trxsig	n_login							
Description	Exchange site	trx signing login							
Supported	ICO CDI								
Interfaces	ISO, SPI								
Supported	02h: NORMA	02h: NORMAL							
Modes	03h: AUTH								
	APDU	80 FB 00 00	LC	44	LE	04			
Command	CDATA	[TRXID] [OKTK]	N] [EN	IC_UB	LKTK	N]			
Specification	CDAIA	[ACCID] [DEAL	AMNT	[MAC	C]				
	RESPONSE	NSE [TRXHANDLE] [SW (2 bytes)							
	TRXID	Transaction ID (4 bytes)							
	OKTKN	OK token (4 bytes)							
	ENC_UBLKTKN	Encrypted unblock token (16 bytes)							
	ACCID	Account ID (4 byt	es, litt	le-endia	an)				
Parameter	DEALAMNT	Deal amount (8 by	tes, bi	ig-endia	ın)				
1 ai ailictei		MAC value of (TI	RXID	OKTK	KN				
	MAC	UBLKTKN ACC	CID 1	DEALA	MNT)			
	MAC	(32 bytes)							
		MAC key is XCHS_S	SK .						
	TRXHANDLE	Transaction signing	g hand	dle (4 b	ytes)				
	• The regist	ration status must b	e REC	GISTER	ED				
	XCHS ses	sion must be establ	ished						
Note	Unblock to	oken (16 bytes) is c	ompos	sed of:					
	■ BYTE	$E[0 \sim 7]$: Prefix							
	■ BYTE	$E[8 \sim 15]$: Amount							

4.11.13. se_xchs_trxsign_prepare

Command	se_xchs_trxsig	n_prepare					
Description	Exchange site	trx signing prepare					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported	02h: NORMA	L					
Modes	03h: AUTH						
	APDU	80 FC [IN_ID] 00					
Command Specification	CDATA	[TRXHANDLE] [ACCID] [KCID] [KID] [OUT1ADDR] [OUT2ADDR] [SIGMTRL] [MAC]					
	RESPONSE	[SW (2 bytes)]					
	TRXHANDLE	Transaction signing handle (4 bytes)					
	IN_ID	Input ID (0 ~ 255)					
	ACCID	Account ID (4 bytes, little-endian)					
		Key chain ID (1 byte)					
	KCID	00h: External key chain					
		01h: Internal key chain					
Parameter	KID	Key ID (4 bytes, little-endian)					
Farameter	OUT1ADDR	Output 1 address (25 bytes)					
	OUT2ADDR	Output 2 address (25 bytes)					
	SIGMTRL	Signature material (32 bytes)					
		MAC value of (ACCID KCID KID					
	MAC	OUT1ADDR OUT2ADDR					
	IVIAC	SIGMTRL) (32 bytes)					
		MAC key is XCHS_SK					
	• The registr	ration status must be REGISTERED					
Note	XCHS ses	sion must be established					
11016	XCHS sig	ning session must be login					
	• IN_ID has	to start from 0, and must be input in serial					

4.11.14. se_xchs_trxsign_logout

Command	se_xchs_trxsig	gn_logout					
Description	Exchange site	Exchange site trx signing logout					
Supported Interfaces	ISO, SPI	ISO, SPI					
Supported	02h: NORMAL						
Modes	03h: AUTH			_			
	APDU	80 FD 00 00 LC 14 LE 50					
Command	CDATA	[TRXHANDLE]	[NON	CE]			
Specification	RESPONSE	[SIGRCPT] [MAG [SW (2 bytes)]	C] [NO	ONCES	E]		
	TRXHANDLE	Transaction signir	ng han	dle (4 b	ytes)		
	NONCE	Nonce for signatu	re rece	eipt (16	bytes)		
	SIGRCPT	Signature receipt	(32 by	tes)			
Parameter	MAC	MAC value of SIGRCPT (32 bytes) MAC key is XCHS_SK					
	NONCESE	Nonce for signature receipt generated by SE (16 bytes)					
Note	 XCHS ses SIGRCPT key is XC CARI UID TRX_ ACC_ DEAI NUM OUT1 	ID _ID AMOUNT _INPUTS ADDR 2ADDR	ished			IAC	

4.12. Credential

4.12.1. se_cred_get_mem

Command	se_cred_get_n	nem						
Description	Get memory c	Get memory credential						
Supported	ICO CDI							
Interfaces	150, 511	SO, SPI						
Supported	All madas	All modes						
Modes	All filodes							
Command	APDU	80 38 00 00	LC	00	LE	25		
0 0 22222022	CDATA	None						
Specification	RESPONSE	[HANDLE] [MEMO	CREC)][SW	(2 byt	tes)]		
Parameter	HANDLE	Memory credential h	nandl	e (4 by	tes)			
rarameter	MEMCRED	IEMCRED Memory credential (33 bytes)						
Note	None							

4.12.2. se_cred_set_mem

Command	se_cred_set_mem					
Description	Restore memory credential					
Supported	ICO CDI	IGO CDI				
Interfaces	ISO, SPI					
Supported	All modes					
Modes						
Commond	APDU	80 39 00 00	LC	25	LE	00
Command	CDATA [HANDLE] [MEMCRED]					
Specification	RESPONSE	RESPONSE [SW (2 bytes)]				
D	HANDLE Memory credential handle (4 bytes) MEMCRED Memory credential (33 bytes)					
Parameter						
Note	None					

4.12.3. se_cred_get_nvm

Command	se_cred_get_nvm					
Description	Get NVM cred	Get NVM credential				
Supported	ICO CDI	IGO GDI				
Interfaces	ISO, SPI					
Supported	All modes					
Modes	All modes					
Commond	APDU	80 3A 00 00	LC	00	LE	04
Command	CDATA	CDATA None				
Specification	RESPONSE [HANDLE] [SW (2 bytes)]					
Parameter	HANDLE NVM credential handle (4 bytes)					
Note	None					

4.12.4. se_cred_set_nvm

Command	se_cred_set_nvm					
Description	Restore NVM	Restore NVM credential				
Supported	ICO CDI	IGO GDI				
Interfaces	130, 311	ISO, SPI				
Supported	All modes					
Modes	All modes					
Commond	APDU 80 39 00 00 LC 04 LE (00			
Command	CDATA	CDATA [HANDLE]				
Specification	RESPONSE [SW (2 bytes)]					
Parameter	HANDLE NVM credential handle (4 bytes)					
Note	None					

5. Supported Commands in Each Mode

5.1.APDU in Each Mode – ISO Interface

The following table lists supported APDU commands for each mode in ISO interface.

Mode	Supported commands			
COMMON	se_get_mode_state	mbox_iso_get_resp		
	se_get_fw_version	se_cred_get_mem		
(All modes)	se_get_unique_id	se_cred_set_mem		
(All modes)	se_get_mod_err	se_cred_get_nvm		
	mbox_iso_send_msg	se_cred_set_nvm		
	se_init_set_data	se_init_vmk_chlng		
INIT	se_init_get_data_hash	se_init_change_vmk		
	se_init_confirm			
	se_bind_reg_info	se_bind_back_nohost		
PERSO	se_bind_reg_approve	se_perso_set_data		
TERSO	se_bind_reg_remove	se_perso_get_data_hash		
	se_bind_logout	se_perso_confirm		
	se_bind_reg_info	se_hdw_set_wa_info		
	se_bind_reg_approve	se_hdw_create_account		
	se_bind_reg_remove	se_hdw_qry_acc_info		
	se_bind_logout	se_hdw_set_acc_info		
	se_perso_back_perso	se_hdw_next_trx_addr		
	se_pin_chlng	se_hdw_prep_trx_sign		
NORMAL	se_pin_auth	se_hdw_init_wallet_gen_confirm		
NORWAL	se_pin_logout	se_hdw_qry_acc_keyinfo		
	se_set_currency	se_set_secpo		
	se_get_currency	se_xchs_reg_status		
	se_get_card_name	se_xchs_reg_init		
	se_set_card_name	se_xchs_reg_finish		
	se_get_secpo	se_xchs_reg_clear		
	se_trx_status	se_xchs_get_otp		

	se_trx_prepare	se_xchs_session_init		
	se_trx_begin	se_xchs_session_estab		
	se_trx_verify_otp	se_xchs_session_logout		
	se_trx_sign	se_xchs_block_info		
	se_trx_get_ctxinfo	se_xchs_block_btc		
	se_trx_finish	se_xchs_cancel_block		
	se_hdw_init_wallet	se_xchs_trxsign_login		
	se_hdw_init_wallet_gen	se_xchs_trxsign_prepare		
	se_hdw_qry_wa_info	se_xchs_trxsign_logout		
	se_bind_reg_info	se_hdw_create_account		
	se_bind_reg_approve	se_hdw_qry_acc_info		
	se_bind_reg_remove	se_hdw_set_acc_info		
	se_pin_change	se_hdw_next_trx_addr		
	se_pin_logout	se_hdw_prep_trx_sign		
	se_set_currency	se_hdw_init_wallet_gen_confirm		
	se_get_currency	se_hdw_qry_acc_keyinfo		
	se_get_card_name	se_xchs_reg_status		
	se_set_card_name	se_xchs_reg_init		
	se_get_secpo	se_xchs_reg_finish		
AUTH	se_set_secpo	se_xchs_reg_clear		
AOIII	se_trx_status	se_xchs_get_otp		
	se_trx_prepare	se_xchs_session_init		
	se_trx_begin	se_xchs_session_estab		
	se_trx_verify_otp	se_xchs_session_logout		
	se_trx_sign	se_xchs_block_info		
	se_trx_get_ctxinfo	se_xchs_block_btc		
	se_trx_finish	se_xchs_cancel_block		
	se_hdw_init_wallet	se_xchs_trxsign_login		
	se_hdw_init_wallet_gen	se_xchs_trxsign_prepare		
	se_hdw_qry_wa_info	se_xchs_trxsign_logout		
	se_hdw_set_wa_info			
	se_bind_reg_info	se_puk_chlng		
LOCK	se_bind_logout	se_pin_unlock		
	se_perso_back_perso			
ERROR				

	se_init_vmk_chlng	se_get_card_name	
	se_init_back_init	se_set_card_name	
	se_bind_reg_init	se_get_secpo	
	se_bind_reg_chlng	se_hdw_qry_wa_info	
NOHOST	se_bind_reg_finish	se_hdw_qry_acc_info	
	se_bind_reg_info	se_set_secpo	
	se_pin_chlng	se_xchs_reg_status	
	se_set_currency	se_xchs_get_otp	
	se_get_currency		
	se_init_vmk_chlng	se_pin_chlng	
	se_init_back_init	se_set_currency	
	se_bind_reg_init	se_get_currency	
	se_bind_reg_chlng	se_get_card_name	
	se_bind_reg_finish	se_set_card_name	
DISCONN	se_bind_reg_info	se_get_secpo	
	se_bind_login_chlng	se_hdw_qry_wa_info	
	se_bind_login	se_hdw_qry_acc_info	
	se_bind_find_hst_id	se_xchs_reg_status	
	se_set_secpo	se_xchs_get_otp	
	se_bind_back_nohost		

5.2.APDU in Each Mode – SPI Interface

The following table lists supported APDU commands for each mode in SPI interface.

Mode	Supported commands			
	se_get_mode_state	mbox_spi_send_resp		
COMPACY	se_get_fw_version	se_cred_get_mem		
COMMON	se_get_unique_id	se_cred_set_mem		
(All modes)	se_get_mod_err	se_cred_get_nvm		
	mbox_spi_get_msg	se_cred_set_nvm		
	se_init_set_data	se_init_vmk_chlng		
INIT	se_init_get_data_hash	se_init_change_vmk		
	se_init_confirm			
	se_bind_reg_info	se_bind_back_nohost		
PERSO	se_bind_reg_approve	se_perso_set_data		
IERSO	se_bind_reg_remove	se_perso_get_data_hash		
	se_bind_logout	se_perso_confirm		
	se_bind_reg_info	se_hdw_set_wa_info		
	se_bind_reg_approve	se_hdw_create_account		
	se_bind_reg_remove	se_hdw_qry_acc_info		
	se_bind_logout	se_hdw_set_acc_info		
	se_perso_back_perso	se_hdw_next_trx_addr		
	se_pin_chlng	se_hdw_prep_trx_sign		
	se_pin_auth	se_hdw_init_wallet_gen_confirm		
NORMAL	se_pin_logout	se_hdw_qry_acc_keyinfo		
NORWIAL	se_set_currency	se_set_secpo		
	se_get_currency	se_xchs_reg_status		
	se_get_card_name	se_xchs_reg_init		
	se_set_card_name	se_xchs_reg_finish		
	se_get_secpo	se_xchs_reg_clear		
	se_trx_status	se_xchs_get_otp		
	se_trx_prepare	se_xchs_session_init		
	se_trx_begin	se_xchs_session_estab		

	se_trx_verify_otp	se_xchs_session_logout
	se_trx_sign	se_xchs_block_info
	se_trx_get_ctxinfo	se_xchs_block_btc
	se_trx_finish	se_xchs_cancel_block
	se_trx_outaddr	se_xchs_trxsign_login
	se_hdw_init_wallet	se_xchs_trxsign_prepare
	se_hdw_init_wallet_gen	se_xchs_trxsign_logout
	se_hdw_qry_wa_info	
	se_bind_reg_info	se_hdw_set_wa_info
	se_bind_reg_approve	se_hdw_create_account
	se_bind_reg_remove	se_hdw_qry_acc_info
	se_pin_change	se_hdw_set_acc_info
	se_pin_logout	se_hdw_next_trx_addr
	se_set_currency	se_hdw_prep_trx_sign
	se_get_currency	se_hdw_init_wallet_gen_confirm
	se_get_card_name	se_hdw_qry_acc_keyinfo
	se_set_card_name	se_xchs_reg_status
	se_get_secpo	se_xchs_reg_init
AUTH	se_set_secpo	se_xchs_reg_finish
AOIII	se_trx_status	se_xchs_reg_clear
	se_trx_prepare	se_xchs_get_otp
	se_trx_begin	se_xchs_session_init
	se_trx_verify_otp	se_xchs_session_estab
	se_trx_sign	se_xchs_session_logout
	se_trx_get_ctxinfo	se_xchs_block_info
	se_trx_finish	se_xchs_block_btc
	se_trx_outaddr	se_xchs_cancel_block
	se_hdw_init_wallet	se_xchs_trxsign_login
	se_hdw_init_wallet_gen	se_xchs_trxsign_prepare
	se_hdw_qry_wa_info	se_xchs_trxsign_logout
	se_bind_reg_info	se_puk_chlng
LOCK	se_bind_logout	se_pin_unlock
	se_perso_back_perso	
ERROR		
NOHOST	se_init_vmk_chlng	se_get_card_name

	se_init_back_init	se_set_card_name		
	se_bind_reg_init	se_get_secpo		
	se_bind_reg_chlng	se_hdw_qry_wa_info		
	se_bind_reg_finish	se_hdw_qry_acc_info		
	se_bind_reg_info	se_set_secpo		
	se_pin_chlng	se_xchs_reg_status		
	se_set_currency	se_xchs_get_otp		
	se_get_currency			
	se_init_vmk_chlng	se_pin_chlng		
	se_init_back_init	se_set_currency		
	se_bind_reg_init	se_get_currency		
	se_bind_reg_chlng	se_get_card_name		
	se_bind_reg_finish	se_set_card_name		
DISCONN	se_bind_reg_info	se_get_secpo		
	se_bind_login_chlng	se_hdw_qry_wa_info		
	se_bind_login	se_hdw_qry_acc_info		
	se_bind_find_hst_id	se_xchs_reg_status		
	se_set_secpo	se_xchs_get_otp		
	se_bind_back_nohost			