

REGISTER_ENCRYPTION

This command is used when full packet encryption is to be implemented.

Device UI Required: Yes

Request Packet

Field	Rule	Type	Min	Max	Value	Comments
FUNCTION_TYPE	R	S	•	•	SECURITY	
COMMAND	R	S	•	•	REGISTER_ENCRYPTION	
KEY	R	E	•	•		The public component of RSA 2048-bit key pair. The value should be DER formatted and base64 encoded. The corresponding private key is stored internally by POS. It is used to decrypt the TERMINAL_KEY returned in the response.
REG_VER	C	L	•	•	1.0 or 2.0 Default is 1.0	1.0 - SHA1 with PKCS padding 2.0 - SHA2 with OAEP padding

Response Packet

Field	Type	Value	Comments
RESPONSE_TEXT	C	Registered MAC_LABEL	
RESULT	C	OK or Error Code	Refer to <Error Section>
RESULT_CODE	N	-1 59001 59020 59040 59051	

Field	Type	Value	Comments
TERMINATION_STATUS	C	SUCCESS or Error Codes	
TERMINAL_KEY	E	Encrypted AES-128 with Public Key	This is the terminal key used to encrypt and decrypt the transaction data. It is Base64 data. The decoded, decrypted TERMINAL_KEY is to be used as the MAC Key when encryption is enabled
MAC_LABEL	C	P_<Random String>	Value to be stored by POS
ENTRY_CODE	C	Value entered by user	Sent in response for POS to validate for REV_VER=2. Appears as Base64 encoded.