

1. Key Identifiers and Constants

This section outlines the specific, hardcoded identifiers used to locate files and objects on the Maltese eID card. These values are crucial for the documentation as they represent the primary differences from a generic specification.

Constant Name	Value (Hex)	Description
DF_AUTH_ID	50 15	Dedicated File (DF) for the authentication key and certificate.
DF_SIG_ID	1F FF	Dedicated File (DF) for the signing key and certificate.
FID_AUTH_CER T	54 02	Elementary File ID (EFID) for the Authentication Certificate.
FID_SIG_CERT	54 01	Elementary File ID (EFID) for the Signing Certificate.
KEY_REF_AUTH	82	Key Reference byte for the authentication private key.
KEY_REF_SIG	81	Key Reference byte for the signing private key.
PIN_REF_AUTH	83	PIN Reference byte for the authentication PIN.
PIN_REF_SIG	82	PIN Reference byte for the signing PIN.

2. Command Set for Maltese eID Card

The following tables describe the APDU commands used in the library. The CLA byte 0x0C is consistently used, indicating that commands are sent over a secure channel established via PACE. The documentation describes the unwrapped command that the card's application layer processes.

2.1 Commands for Selection

The SELECT command is used to set the current context to a specific file, either a Dedicated File (DF) or an Elementary File (EF).

Table 1 — SELECT command-response pair

Command Parameter	Value (Hex)	Meaning
CLA	0C	Secure messaging, logical channel 0.
INS	A4	SELECT
P1	See Table 2	Selection type.
P2	0C	No response data expected in the data field of the command.
Lc field	Present	Length of the command data field.
Data field	See Table 2	File Identifier (DF Name or EFID).
Le field	Absent	N/A

Response Parameter	Meaning
Data field	File control information (FCI)
SW1-SW2	9000 (Success), 6283 (File invalidated), 6A82 (File not found)

Table 2 — P1 and Data Field values for SELECT

P1	Data Field	Description
0	50 15 or 1F FF	Select by DF Name. This is used to select either the Authentication or Signing Dedicated File.
2	54 02 or 54 01	Select EF under current DF. Used to select the certificate file after its parent DF has been selected.

2.2 Commands for Data Unit Handling

The READ BINARY command is used to read the content of the currently selected Elementary File (e.g., a certificate). The implementation reads the file in chunks.

Table 3 — READ BINARY command-response pair

Command Parameter	Value (Hex)	Meaning
CLA	0C	Secure messaging, logical channel 0.
INS	B0	READ BINARY
P1-P2	Offset	Offset of the data to be read, encoded in 2 bytes (big-endian). E.g., 00 00 for the start.
Lc field	Absent	N/A
Le field	C8 (200)	Length of data expected in response. The library requests chunks of 200 bytes.
Response Parameter	Meaning	
Data field	The bytes read from the file.	
SW1-SW2	9000 (Success), 6282 (End of file reached), 6B00 (Wrong parameter P1-P2, offset invalid)	

2.3 Commands for Basic Security Handling

The VERIFY command is used to perform PIN verification. This must be done successfully before any private key operation can be performed.

Table 4 — VERIFY command-response pair

Command Parameter	Value (Hex)	Meaning
CLA	0C	Secure messaging, logical channel 0.
INS	20	VERIFY
P1	0	No specific verification information.
P2	See below	Reference of the PIN to be verified (83 for Auth, 82 for Sig).
Lc field	6	Length of the 6-digit PIN.
Data field	<i>PIN</i>	The 6-digit PIN encoded in ISO-8859-1.
Le field	Absent	N/A

Response Parameter	Meaning
Data field	Absent
SW1-SW2	9000 (Success), 63CX (Verification failed, X retries left), 6983 (PIN blocked)

2.4 Commands for Security Operations

The MSE:SET command is used to set the security environment for a subsequent cryptographic operation. It tells the card which key and which signature algorithm to use.

Table 5 — MSE:SET command-response pair

Command Parameter	Value (Hex)	Meaning
CLA	0C	Secure messaging, logical channel 0.
INS	22	MANAGE SECURITY ENVIRONMENT
P1	41	SET mode
P2	B6	Digital Signature Template
Lc field	6	Length of the command data.
Data field	See Table 6	Control Reference Template data.
Le field	Absent	N/A

Response Parameter	Meaning
Data field	Absent
SW1-SW2	9000 (Success)

Table 6 — Data Field for MSE:SET

The data field is a concatenation of two Data Objects (DOs):

Algorithm Reference (Tag 80): Specifies the signature algorithm.

Key Reference (Tag 84): Specifies the private key to be used.

Example for Signing with RSA-PSS:

80 01 EC 84 01 81

Tag	Length	Value	Description
80	1	EC	Algorithm: RSASSA-PSS
84	1	81	Key: Signing Private Key (Ref 81)

Example for Authentication with PKCS1-v1.5:

80 01 E8 84 01 82

Tag	Length	Value	Description
80	1	E8	Algorithm: RSASSA-PKCS1-v1_5
84	1	82	Key: Authentication Private Key (Ref 82)

This command instructs the card to compute a digital signature on a given hash. It uses the context established by the preceding MSE:SET command.

Table 7 — PSO:COMPUTE DIGITAL SIGNATURE command-response pair

Command Parameter	Value (Hex)	Meaning
CLA	0C	Secure messaging, logical channel 0.
INS	2A	PERFORM SECURITY OPERATION
P1	9E	Digital Signature
P2	9A	Compute
Lc field	20	Length of the SHA-256 hash (32 bytes).
Data field	<i>Hash</i>	The 32-byte SHA-256 hash to be signed.
Le field	0	The library sends Le=0x256 (encoded as 00). Note: This is a key implementation-specific detail for the Maltese card to avoid a 6700 (Wrong Length) error.