# i.MX8 SHE API

Revision\_1.0

Generated by Doxygen 1.8.15

1	Module Index	1
	1.1 Modules	1
2	Module Documentation	2
	2.1 Error codes	2
	2.1.1 Detailed Description	2
	2.1.2 Enumeration Type Documentation	2
	2.2 SHE keys	
	2.2.1 Detailed Description	4
	2.3 SHE+ key extension	
	2.3.1 Detailed Description	5
	2.4 Key store provisioning	6
	2.4.1 Detailed Description	6
	2.4.2 Function Documentation	6
	2.5 Session	8
	2.5.1 Detailed Description	8
	2.5.2 Function Documentation	8
	2.6 SHE commands	9
	2.6.1 Detailed Description	9
	2.7 CMD_GENERATE_MAC	10
	2.7.1 Detailed Description	10
	2.7.2 Function Documentation	10
	2.8 CMD_VERIFY_MAC	11
	2.8.1 Detailed Description	11
	2.8.2 Function Documentation	11
	2.9 CMD_ENC_CBC	12
	2.9.1 Detailed Description	12
	2.9.2 Function Documentation	12
	2.10 CMD_DEC_CBC	13
	2.10.1 Detailed Description	13
	2.10.2 Function Documentation	13
	2.11 CMD_ENC_ECB	14
	2.11.1 Detailed Description	14
	2.11.2 Function Documentation	14
	2.12 CMD_DEC_ECB	15
	2.12.1 Detailed Description	15
	2.12.2 Function Documentation	15
	2.13 CMD_LOAD_KEY	16
	2.13.1 Detailed Description	16
	2.13.2 Function Documentation	16
	2.14 CMD_LOAD_PLAIN_KEY	17
	2.14.1 Detailed Description	17

1 Module Index

2.14.2 Function Documentation	 	17
2.15 CMD_EXPORT_RAM_KEY	 	18
2.15.1 Detailed Description	 	18
2.15.2 Function Documentation	 	18
2.16 CMD_INIT_RNG	 	19
2.16.1 Detailed Description	 	19
2.16.2 Function Documentation	 	19
2.17 CMD_EXTEND_SEED		20
2.17.1 Detailed Description	 	20
2.17.2 Function Documentation		20
2.18 CMD_RND		21
2.18.1 Detailed Description		21
2.18.2 Function Documentation		21
2.19 CMD_GET_STATUS		22
2.19.1 Detailed Description		22
2.19.2 Function Documentation		22
2.20 CMD_GET_ID		23
2.20.1 Detailed Description		23
2.20.2 Function Documentation		23 24
2.21 CMD_CANCEL		24
2.21.1 Detailed Description		24
2.21.21 unction bocumentation	 	24
Index		25
4 Madula Inday		
1 Module Index		
1.1 Modules		
Here is a list of all modules:		
nere is a list of all modules.		
Error codes		2
SHE keys		4
SHE+ key extension		5
Key store provisioning		6
Session		8
SHE commands		9
CMD_GENERATE_MAC		10
CMD_VERIFY_MAC		11
CMD_ENC_CBC		12
05_E110_0B0		14

CMD_DEC_CBC	13
CMD_ENC_ECB	14
CMD_DEC_ECB	15
CMD_LOAD_KEY	16
CMD_LOAD_PLAIN_KEY	17
CMD_EXPORT_RAM_KEY	18
CMD_INIT_RNG	19
CMD_EXTEND_SEED	20
CMD_RND	21
CMD_GET_STATUS	22
CMD_GET_ID	23
CMD_CANCEL	24

### 2 Module Documentation

### 2.1 Error codes

### **Enumerations**

```
enum she_err_t {
    ERC_NO_ERROR = 0x0,
    ERC_SEQUENCE_ERROR = 0x1,
    ERC_KEY_NOT_AVAILABLE = 0x2,
    ERC_KEY_INVALID = 0x3,
    ERC_KEY_EMPTY = 0x4,
    ERC_NO_SECURE_BOOT = 0x5,
    ERC_KEY_WRITE_PROTECTED = 0x6,
    ERC_KEY_UPDATE_ERROR = 0x7,
    ERC_RNG_SEED = 0x8,
    ERC_NO_DEBUGGING = 0x9,
    ERC_BUSY = 0xA,
    ERC_MEMORY_FAILURE = 0xB,
    ERC_GENERAL_ERROR = 0xC }
```

### 2.1.1 Detailed Description

Error codes returned by SHE functions.

### 2.1.2 Enumeration Type Documentation

### 2.1.2.1 she\_err\_t

enum she\_err\_t

2.1 Error codes

### Enumerator

ERC_NO_ERROR	Success.
ERC_SEQUENCE_ERROR	Invalid sequence of commands.
ERC_KEY_NOT_AVAILABLE	Key is locked.
ERC_KEY_INVALID	Key not allowed for the given operation.
ERC_KEY_EMPTY	Key has not beed initialized yet.
ERC_NO_SECURE_BOOT	Conditions for a secure boot process are not met.
ERC_KEY_WRITE_PROTECTED	Memory slot for this key has been write-protected.
ERC_KEY_UPDATE_ERROR	Key update did not succeed due to errors in verification of the messages.
ERC_RNG_SEED	The seed has not been initialized.
ERC_NO_DEBUGGING	Internal debugging is not possible.
ERC_BUSY	A function of SHE is called while another function is still processing.
ERC_MEMORY_FAILURE	Memory error (e.g. flipped bits)
ERC_GENERAL_ERROR	Error not covered by other codes occured.

## 2.2 SHE keys

### Macros

- #define **SHE\_KEY\_1** (0x04)
- #define **SHE\_KEY\_2** (0x05)
- #define SHE\_KEY\_3 (0x06)
- #define **SHE\_KEY\_4** (0x07)
- #define **SHE\_KEY\_5** (0x08)
- #define **SHE\_KEY\_6** (0x09)
- #define SHE\_KEY\_7 (0x0a)
- #define SHE\_KEY\_8 (0x0b)
- #define SHE\_KEY\_9 (0x0c)
- #define **SHE\_KEY\_10** (0x0d)
- #define **SHE\_RAM\_KEY** (0x0e)

### 2.2.1 Detailed Description

Identifiers for SHE keys.

### 2.3 SHE+ key extension

#### Macros

```
#define SHE_KEY_DEFAULT (0x00)
no key extension: keys from 0 to 10 as defined in SHE specification.
#define SHE_KEY_N_EXT_1 (0x10)
keys 11 to 20.
#define SHE_KEY_N_EXT_2 (0x20)
keys 21 to 30.
#define SHE_KEY_N_EXT_3 (0x30)
keys 31 to 40.
#define SHE_KEY_N_EXT_4 (0x40)
keys 41 to 50.
```

### 2.3.1 Detailed Description

Identifiers for the SHE key extension.

### 2.4 Key store provisioning

#### Macros

• #define SHE\_STORAGE\_CREATE\_SUCCESS 0u

New storage created succesfully.

· #define SHE STORAGE CREATE WARNING 1u

New storage created but its usage is restricted to a limited security state of the chip.

• #define SHE\_STORAGE\_CREATE\_UNAUTHORIZED 2u

Creation of the storage is not authorized.

• #define SHE\_STORAGE\_CREATE\_FAIL 3u

Creation of the storage failed for any other reason.

• #define SHE\_STORAGE\_NUMBER\_UPDATES\_DEFAULT 300u

default number of maximum number of updated for SHE storage.

### **Functions**

uint32\_t she\_storage\_create (uint32\_t key\_storage\_identifier, uint32\_t authentication\_nonce, uint16\_t max
 —updates\_number, uint8\_t \*signed\_message, uint32\_t msg\_len)

### 2.4.1 Detailed Description

### 2.4.2 Function Documentation

#### 2.4.2.1 she\_storage\_create()

Creates an empty SHE storage.

Must be called at least once on every device before using any other SHE API.

A signed message must be provided to replace an existing key store. This message is not necessary under some conditions related to chip's lifecycle.

Note that the signed message is not yet supported. should be forced to NULL.

### **Parameters**

kov storago identifior	kov storo idantifiar
key_storage_identifier	key store identifier
authentication_nonce	user defined nonce to be used as authentication proof for accesing the key store.
max_updates_number	maximum number of updates authorized on this new storage.  This parameter has the goal to limit the occupation of the monotonic counter used as anti-rollback protection.  If the maximum number of updates is reached, SHE still allows key store updates but without updating the monotonic counter giving the opportunity for rollback attacks.  Always forced to 300 in the current release.
signed_message	pointer to a signed message authorizing the operation (NULL if no signed message to be used)
msg_len	length in bytes of the signed message

Returns

### 2.5 Session

#### **Functions**

- struct she\_hdl\_s \* she\_open\_session (uint32\_t key\_storage\_identifier, uint32\_t authentication\_nonce, void(\*async\_cb)(void \*priv, she\_err\_t err), void \*priv)
- void she close session (struct she hdl s \*hdl)

### 2.5.1 Detailed Description

#### 2.5.2 Function Documentation

### 2.5.2.1 she\_open\_session()

Initiate a SHE session. The returned session handle pointer is typed with the struct "she\_hdl\_s". The user doesn't need to know or to access the fields of this struct.

It only needs to store this pointer and pass it to every calls to other APIs within the same SHE session.

Note that asynchronous API is currently not supported. async\_cb and priv pointers must be set to NULL.

### Parameters

key_storage_identifier	key store identifier
authentication_nonce	user defined nonce used as authentication proof for accesing the key store
async_cb	user callback to be called on completion of a SHE operation
priv	user pointer to be passed to the callback

### Returns

pointer to the session handle.

### 2.5.2.2 she\_close\_session()

Terminate a previously opened SHE session

### **Parameters**

hdl pointer to the session handler to be closed.

2.6 SHE commands 9

### 2.6 SHE commands

### Modules

- CMD\_GENERATE\_MAC
- CMD\_VERIFY\_MAC
- CMD\_ENC\_CBC
- CMD\_DEC\_CBC
- CMD\_ENC\_ECB
- CMD\_DEC\_ECB
- CMD\_LOAD\_KEY
- CMD\_LOAD\_PLAIN\_KEY
- CMD\_EXPORT\_RAM\_KEY
- CMD\_INIT\_RNG
- CMD\_EXTEND\_SEED
- CMD\_RND
- CMD\_GET\_STATUS
- CMD\_GET\_ID
- CMD\_CANCEL

### 2.6.1 Detailed Description

## 2.7 CMD\_GENERATE\_MAC

#### Macros

#define SHE\_MAC\_SIZE 16u
 size of the MAC generated is 128bits.

### **Functions**

- she\_err\_t she\_cmd\_generate\_mac (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint16\_← t message\_length, uint8\_t \*message, uint8\_t \*mac)
- 2.7.1 Detailed Description
- 2.7.2 Function Documentation

### 2.7.2.1 she\_cmd\_generate\_mac()

Generates a MAC of a given message with the help of a key identified by key\_id.

### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
message_length	lenght in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE.
message	pointer to the message to be processed
mac	pointer to where the output MAC should be written (128bits should be allocated there)

### Returns

### 2.8 CMD\_VERIFY\_MAC

#### Macros

- #define SHE\_MAC\_VERIFICATION\_SUCCESS 0u indication of mac verification success
- #define SHE\_MAC\_VERIFICATION\_FAILED 1u

indication of mac verification failure

#### **Functions**

she\_err\_t she\_cmd\_verify\_mac (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint16\_t message\_
 length, uint8\_t \*message, uint8\_t \*mac, uint8\_t mac\_length, uint8\_t \*verification\_status)

#### 2.8.1 Detailed Description

#### 2.8.2 Function Documentation

### 2.8.2.1 she\_cmd\_verify\_mac()

```
she_err_t she_cmd_verify_mac (
    struct she_hdl_s * hdl,
    uint8_t key_ext,
    uint8_t key_id,
    uint16_t message_length,
    uint8_t * message,
    uint8_t * mac,
    uint8_t * mac_length,
    uint8_t * verification_status )
```

Verifies the MAC of a given message with the help of a key identified by key\_id.

### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
message_length	lenght in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE.
message	pointer to the message to be processed
mac	pointer to the MAC to be compared (implicitely 128 bits)
mac_length	number of bytes to compare (must be at least 4)
verification_status	pointer to where write the result of the MAC comparison

#### Returns

### 2.9 CMD\_ENC\_CBC

#### Macros

#define SHE\_AES\_BLOCK\_SIZE\_128 16u
 size in bytes of a 128bits CBC block

### **Functions**

• she\_err\_t she\_cmd\_enc\_cbc (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint32\_t data\_length, uint8\_t \*iv, uint8\_t \*plaintext, uint8\_t \*ciphertext)

### 2.9.1 Detailed Description

### 2.9.2 Function Documentation

### 2.9.2.1 she\_cmd\_enc\_cbc()

CBC encryption of a given plaintext with the key identified by key\_id.

### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
data_length	lenght in bytes of the plaintext and the cyphertext. Must be a multiple of 128bits.
iv	pointer to the 128bits IV to use for the encryption.
plaintext	pointer to the message to be encrypted.
ciphertext	pointer to ciphertext output area.

### Returns

2.10 CMD DEC CBC

### 2.10 CMD\_DEC\_CBC

### **Functions**

• she\_err\_t she\_cmd\_dec\_cbc (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint32\_t data\_length, uint8\_t \*iv, uint8\_t \*ciphertext, uint8\_t \*plaintext)

- 2.10.1 Detailed Description
- 2.10.2 Function Documentation

### 2.10.2.1 she\_cmd\_dec\_cbc()

CBC decryption of a given ciphertext with the key identified by key\_id.

#### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
data_length	lenght in bytes of the plaintext and the cyphertext. Must be a multiple of 128bits.
iv	pointer to the 128bits IV to use for the decryption.
ciphertext	pointer to ciphertext to be decrypted.
plaintext	pointer to the plaintext output area.

### Returns

### 2.11 CMD\_ENC\_ECB

### **Functions**

• she\_err\_t she\_cmd\_enc\_ecb (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint8\_t \*plaintext, uint8\_t \*ciphertext)

### 2.11.1 Detailed Description

### 2.11.2 Function Documentation

### 2.11.2.1 she\_cmd\_enc\_ecb()

ECB encryption of a given plaintext with the key identified by key\_id.

### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
plaintext	pointer to the 128bits message to be encrypted.
ciphertext	pointer to ciphertext output area (128bits).

### Returns

2.12 CMD DEC ECB 15

## 2.12 CMD\_DEC\_ECB

### **Functions**

• she\_err\_t she\_cmd\_dec\_ecb (struct she\_hdl\_s \*hdl, uint8\_t key\_ext, uint8\_t key\_id, uint8\_t \*ciphertext, uint8\_t \*plaintext)

- 2.12.1 Detailed Description
- 2.12.2 Function Documentation
- 2.12.2.1 she\_cmd\_dec\_ecb()

ECB decryption of a given ciphertext with the key identified by key\_id.

### **Parameters**

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
ciphertext	pointer to 128bits ciphertext to be decrypted.
plaintext	pointer to the plaintext output area (128bits).

### Returns

### 2.13 CMD\_LOAD\_KEY

#### Macros

```
    #define SHE_KEY_SIZE 16u
    SHE keys are 128 bits (16 bytes) long.
```

### **Functions**

```
• she_err_t she_cmd_load_key (struct she_hdl_s *hdl, uint8_t key_ext, uint8_t key_id, uint8_t *m1, uint8_t *m2, uint8_t *m3, uint8_t *m4, uint8_t *m5)
```

### 2.13.1 Detailed Description

### 2.13.2 Function Documentation

### 2.13.2.1 she\_cmd\_load\_key()

Update an internal key of SHE with the protocol specified by SHE.

### Parameters

hdl	pointer to the SHE session handler
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
m1	pointer to M1 message - 128 bits
m2	pointer to M2 message - 256 bits
m3	pointer to M3 message - 128 bits
m4	pointer to the output address for M4 message - 256 bits
m5	pointer to the output address for M5 message - 128 bits

### Returns

## 2.14 CMD\_LOAD\_PLAIN\_KEY

### **Functions**

```
• she_err_t she_cmd_load_plain_key (struct she_hdl_s *hdl, uint8_t *key)
```

- 2.14.1 Detailed Description
- 2.14.2 Function Documentation
- 2.14.2.1 she\_cmd\_load\_plain\_key()

Load a key as plaintext to the RAM\_KEY slot without encryption and verification.

### **Parameters**

	hdl	pointer to the SHE session handler
Ī	key	pointer to the plaintext key to be loaded - 128bits

### Returns

## 2.15 CMD\_EXPORT\_RAM\_KEY

### **Functions**

```
• she_err_t she_cmd_export_ram_key (struct she_hdl_s *hdl, uint8_t *m1, uint8_t *m2, uint8_t *m3, uint8_t *m4, uint8_t *m5)
```

- 2.15.1 Detailed Description
- 2.15.2 Function Documentation
- 2.15.2.1 she\_cmd\_export\_ram\_key()

exports the RAM\_KEY into a format protected by SECRET\_KEY.

### **Parameters**

hdl	pointer to the SHE session handler
m1	pointer to the output address for M1 message - 128 bits
m2	pointer to the output address for M2 message - 256 bits
тЗ	pointer to the output address for M3 message - 128 bits
m4	pointer to the output address for M4 message - 256 bits
m5	pointer to the output address for M5 message - 128 bits

### Returns

2.16 CMD INIT RNG 19

## 2.16 CMD\_INIT\_RNG

**Functions** 

```
• she_err_t she_cmd_init_rng (struct she_hdl_s *hdl)
```

- 2.16.1 Detailed Description
- 2.16.2 Function Documentation

```
2.16.2.1 she_cmd_init_rng()
```

initializes the seed and derives a key for the PRNG. The function must be called before CMD\_RND after every power cycle/reset.

### **Parameters**

hdl pointer to the SHE session handler

Returns

### 2.17 CMD\_EXTEND\_SEED

#### Macros

• #define SHE\_ENTROPY\_SIZE 16u

#### **Functions**

```
• she_err_t she_cmd_extend_seed (struct she_hdl_s *hdl, uint8_t *entropy)
```

- 2.17.1 Detailed Description
- 2.17.2 Function Documentation
- 2.17.2.1 she\_cmd\_extend\_seed()

extends the seed of the PRNG by compressing the former seed value and the supplied entropy into a new seed which will be used to generate the following random numbers. The random number generator has to be initialized by CMD\_INIT\_RNG before the seed can be extended.

#### **Parameters**

hdl	pointer to the SHE session handler
entropy	pointer to the entropy vector (128bits) to use for the operation

### Returns

2.18 CMD RND 21

### 2.18 CMD\_RND

Macros

• #define SHE\_RND\_SIZE 16u

### **Functions**

```
• she_err_t she_cmd_rnd (struct she_hdl_s *hdl, uint8_t *rnd)
```

- 2.18.1 Detailed Description
- 2.18.2 Function Documentation
- 2.18.2.1 she\_cmd\_rnd()

returns a vector of 128 random bits. The random number generator has to be initialized by CMD\_INIT\_RNG before random numbers can be supplied.

### **Parameters**

hdl	pointer to the SHE session handler	
rnd	pointer to the output address for the generated 128bits random vector	

Returns

## 2.19 CMD\_GET\_STATUS

### **Functions**

```
• she_err_t she_cmd_get_status (struct she_hdl_s *hdl, uint8_t *sreg)
```

- 2.19.1 Detailed Description
- 2.19.2 Function Documentation

### 2.19.2.1 she\_cmd\_get\_status()

returns the content of the status register

### **Parameters**

hdl	pointer to the SHE session handler
sreg	pointer to the output address for status register(8bits)

### Returns

2.20 CMD GET\_ID 23

### 2.20 CMD\_GET\_ID

#### Macros

- #define SHE\_CHALLENGE\_SIZE 16u /\* 128 bits \*/
- #define **SHE\_ID\_SIZE** 15u /\* 120 bits \*/

### **Functions**

she\_err\_t she\_cmd\_get\_id (struct she\_hdl\_s \*hdl, uint8\_t \*challenge, uint8\_t \*id, uint8\_t \*sreg, uint8\_←
t \*mac)

### 2.20.1 Detailed Description

2.20.2 Function Documentation

## 2.20.2.1 she\_cmd\_get\_id()

returns the identity (UID) and the value of the status register protected by a MAC over a challenge and the data.

### **Parameters**

hdl	pointer to the SHE session handler
challenge	pointer to the challenge vector (128bits)
id	pointer to the output address for the identity (120bits)
sreg	pointer to the output address for status register(8bits)
mac	pointer to the output address for the computed MAC (128bits)

### Returns

## 2.21 CMD\_CANCEL

**Functions** 

```
• she_err_t she_cmd_cancel (struct she_hdl_s *hdl)
```

- 2.21.1 Detailed Description
- 2.21.2 Function Documentation

```
2.21.2.1 she_cmd_cancel()
```

interrupt any given function and discard all calculations and results.

### **Parameters**

hdl pointer to the SHE session handler

### Returns

# Index

CMD_CANCEL, 24	ERC_SEQUENCE_ERROR
she_cmd_cancel, 24	Error codes, 3
CMD_DEC_CBC, 13	Error codes, 2
she_cmd_dec_cbc, 13	ERC_BUSY, 3
CMD DEC ECB, 15	ERC_GENERAL_ERROR, 3
she_cmd_dec_ecb, 15	ERC KEY EMPTY, 3
CMD ENC CBC, 12	ERC_KEY_INVALID, 3
she_cmd_enc_cbc, 12	ERC_KEY_NOT_AVAILABLE, 3
CMD_ENC_ECB, 14	ERC KEY UPDATE ERROR, 3
she cmd enc ecb, 14	ERC KEY WRITE PROTECTED, 3
CMD_EXPORT_RAM_KEY, 18	ERC MEMORY FAILURE, 3
she_cmd_export_ram_key, 18	ERC_NO_DEBUGGING, 3
CMD_EXTEND_SEED, 20	ERC_NO_ERROR, 3
she_cmd_extend_seed, 20	ERC_NO_SECURE_BOOT, 3
CMD_GENERATE_MAC, 10	ERC_RNG_SEED, 3
she_cmd_generate_mac, 10	ERC_SEQUENCE_ERROR, 3
CMD GET ID, 23	she_err_t, 2
she_cmd_get_id, 23	/
CMD_GET_STATUS, 22	Key store provisioning, 6
she_cmd_get_status, 22	she_storage_create, 6
CMD_INIT_RNG, 19	
	Session, 8
she_cmd_init_rng, 19	she_close_session, 8
CMD_LOAD_KEY, 16	she_open_session, 8
she_cmd_load_key, 16	SHE commands, 9
CMD_LOAD_PLAIN_KEY, 17	SHE keys, 4
she_cmd_load_plain_key, 17	SHE+ key extension, 5
CMD_RND, 21	she_close_session
she_cmd_rnd, 21	Session, 8
CMD_VERIFY_MAC, 11	she_cmd_cancel
she_cmd_verify_mac, 11	CMD_CANCEL, 24
	she_cmd_dec_cbc
ERC_BUSY	CMD_DEC_CBC, 13
Error codes, 3	she_cmd_dec_ecb
ERC_GENERAL_ERROR	CMD_DEC_ECB, 15
Error codes, 3	she_cmd_enc_cbc
ERC_KEY_EMPTY	CMD_ENC_CBC, 12
Error codes, 3	she_cmd_enc_ecb
ERC_KEY_INVALID	CMD_ENC_ECB, 14
Error codes, 3	she_cmd_export_ram_key
ERC_KEY_NOT_AVAILABLE	CMD_EXPORT_RAM_KEY, 18
Error codes, 3	she_cmd_extend_seed
ERC_KEY_UPDATE_ERROR	CMD_EXTEND_SEED, 20
Error codes, 3	she_cmd_generate_mac
ERC_KEY_WRITE_PROTECTED	CMD_GENERATE_MAC, 10
Error codes, 3	she_cmd_get_id
ERC_MEMORY_FAILURE	CMD_GET_ID, 23
Error codes, 3	she_cmd_get_status
ERC_NO_DEBUGGING	CMD GET STATUS, 22
Error codes, 3	she_cmd_init_rng
ERC_NO_ERROR	CMD_INIT_RNG, 19
Error codes, 3	she_cmd_load_key
ERC_NO_SECURE_BOOT	CMD_LOAD_KEY, 16
Error codes, 3	she_cmd_load_plain_key
ERC_RNG_SEED	CMD_LOAD_PLAIN_KEY, 17
Error codes, 3	she_cmd_rnd
, -	

26 INDEX