

# i.MX8 HSM API

Revision\_0.1

Generated by Doxygen 1.8.15

<b>1 Main Page</b>	<b>1</b>
<b>1 Main Page</b>	<b>1</b>
<b>2 History</b>	<b>1</b>
<b>3 Module Index</b>	<b>1</b>
3.1 Modules . . . . .	1
<b>4 Module Documentation</b>	<b>1</b>
4.1 Hsm_api . . . . .	1
4.1.1 Detailed Description . . . . .	3
4.1.2 Macro Definition Documentation . . . . .	3
4.1.3 Enumeration Type Documentation . . . . .	5
4.1.4 Function Documentation . . . . .	6
<b>Index</b>	<b>11</b>

## 1 Main Page

This document is a software referece description of the API provided by the i.MX8 HSM solutions.

## 2 History

Revision 0.1: 29/03/2019 Savari preliminary draft - subject to change

## 3 Module Index

### 3.1 Modules

Here is a list of all modules:

<b>Hsm_api</b>	<b>1</b>
----------------	----------

## 4 Module Documentation

### 4.1 Hsm\_api

i.MX8 HSM API header file

## Macros

- `#define HSM_KEY_STORAGE_ACCESS_FLAG_NEW (1 << 0)`
- `#define HSM_KEY_IDENTIFIER_NEW 0xFFFFFFFF`
- `#define HSM_KEY_TYPE_ECDSA_NIST_P224 0x00`
- `#define HSM_KEY_TYPE_ECDSA_NIST_P256 0x01`
- `#define HSM_KEY_TYPE_ECDSA_NIST_P384 0x02`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_224 0x10`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_256 0x11`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_384 0x12`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_224 0x20`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_256 0x21`
- `#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_384 0x22`
- `#define HSM_KEY_TYPE_AES_128 0x30`
- `#define HSM_KEY_TYPE_AES_192 0x31`
- `#define HSM_KEY_TYPE_AES_256 0x32`
- `#define HSM_KEY_FLAGS_TRANSIENT (1 << 0)`
- `#define HSM_KEY_FLAGS_PERMANENT (1 << 1)`
- `#define HSM_CIPHER_ONE_GO_ALGO_AES_ECB 0x00`
- `#define HSM_CIPHER_ONE_GO_ALGO_AES_CBC 0x01`
- `#define HSM_CIPHER_ONE_GO_FLAGS_ENCRYPT (1)`
- `#define HSM_CIPHER_ONE_GO_FLAGS_DECRYPT (0)`

## Enumerations

- `enum hsm_err_t {`  
`HSM_NO_ERROR = 0x0,`  
`HSM_OUT_OF_MEM = 0x1,`  
`HSM_UNKNOWN_HANDLE = 0x2,`  
`HSM_UNKNOWN_KEY_STORE = 0x3,`  
`HSM_KEY_STORE_AUTH_ERROR = 0x4,`  
`HSM_UNKNOWN_ID = 0x5,`  
`HSM_BUF_SIZE_ERROR = 0x6,`  
`HSM_KEY_ERROR = 0x7,`  
`HSM_MEM_ACCESS_ERROR = 0x8,`  
`HSM_INVALID_PARAM = 0x9,`  
`HSM_GENERAL_ERROR = 0xFF }`

*Error codes returned by HSM functions.*

## Functions

- `struct hsm_hdl_s * hsm_open_session (uint32_t key_storage_identifier, uint8_t access_flags, uint32_t password, uint8_t session_priority, uint8_t operating_mode)`
- `hsm_err_t hsm_close_session (struct hsm_hdl_s *hdl)`
- `hsm_err_t hsm_open_key_management_service (struct hsm_hdl_s *hdl, uint32_t input_address_ext, uint32_t output_address_ext)`
- `hsm_err_t hsm_key_management_cmd_key_generation (struct hsm_hdl_s *hdl, uint8_t *key_identifier, uint8_t *output, uint16_t key_type, uint8_t output_size, uint8_t flags)`
- `hsm_err_t hsm_close_key_management_service (struct hsm_hdl_s *hdl)`
- `hsm_err_t hsm_open_cipher_service (struct hsm_hdl_s *hdl, uint32_t input_address_ext, uint32_t output_address_ext, uint8_t flags)`
- `hsm_err_t hsm_cipher_cmd_cipher_one_go (struct hsm_hdl_s *hdl, uint32_t key_identifier, uint8_t *input, uint8_t *output, uint8_t *iv, uint32_t *input_size, uint16_t iv_size, uint8_t algorithm, uint8_t flags)`
- `hsm_err_t hsm_close_cipher_service (struct hsm_hdl_s *hdl)`

#### 4.1.1 Detailed Description

i.MX8 HSM API header file

#### 4.1.2 Macro Definition Documentation

##### 4.1.2.1 HSM\_KEY\_STORAGE\_ACCESS\_FLAG\_NEW

```
#define HSM_KEY_STORAGE_ACCESS_FLAG_NEW (1 << 0)
```

It must be specified to create a new key storage

##### 4.1.2.2 HSM\_KEY\_IDENTIFIER\_NEW

```
#define HSM_KEY_IDENTIFIER_NEW 0xFFFFFFFF
```

It must be specified to create a new key slot

##### 4.1.2.3 HSM\_KEY\_TYPE\_ECDSA\_NIST\_P224

```
#define HSM_KEY_TYPE_ECDSA_NIST_P224 0x00
```

##### 4.1.2.4 HSM\_KEY\_TYPE\_ECDSA\_NIST\_P256

```
#define HSM_KEY_TYPE_ECDSA_NIST_P256 0x01
```

##### 4.1.2.5 HSM\_KEY\_TYPE\_ECDSA\_NIST\_P384

```
#define HSM_KEY_TYPE_ECDSA_NIST_P384 0x02
```

##### 4.1.2.6 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_224

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_224 0x10
```

##### 4.1.2.7 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_256

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_256 0x11
```

**4.1.2.8 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_384**

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_R1_384 0x12
```

**4.1.2.9 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_224**

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_224 0x20
```

**4.1.2.10 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_256**

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_256 0x21
```

**4.1.2.11 HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_384**

```
#define HSM_KEY_TYPE_ECDSA_BRAINPOOL_T1_384 0x22
```

**4.1.2.12 HSM\_KEY\_TYPE\_AES\_128**

```
#define HSM_KEY_TYPE_AES_128 0x30
```

**4.1.2.13 HSM\_KEY\_TYPE\_AES\_192**

```
#define HSM_KEY_TYPE_AES_192 0x31
```

**4.1.2.14 HSM\_KEY\_TYPE\_AES\_256**

```
#define HSM_KEY_TYPE_AES_256 0x32
```

**4.1.2.15 HSM\_KEY\_FLAGS\_TRANSIENT**

```
#define HSM_KEY_FLAGS_TRANSIENT (1 << 0)
```

When set, the key is transient. Transient keys are deleted when the corresponding key store service flow is closed.

**4.1.2.16 HSM\_KEY\_FLAGS\_PERMANENT**

```
#define HSM_KEY_FLAGS_PERMANENT (1 << 1)
```

When set, the key is permanent. Once created, it will not be possible to update or delete the key anymore.

## 4.1.2.17 HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_ECB

```
#define HSM_CIPHER_ONE_GO_ALGO_AES_ECB 0x00
```

## 4.1.2.18 HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_CBC

```
#define HSM_CIPHER_ONE_GO_ALGO_AES_CBC 0x01
```

## 4.1.2.19 HSM\_CIPHER\_ONE\_GO\_FLAGS\_ENCRYPT

```
#define HSM_CIPHER_ONE_GO_FLAGS_ENCRYPT (1)
```

## 4.1.2.20 HSM\_CIPHER\_ONE\_GO\_FLAGS\_DECRYPT

```
#define HSM_CIPHER_ONE_GO_FLAGS_DECRYPT (0)
```

## 4.1.3 Enumeration Type Documentation

## 4.1.3.1 hsm\_err\_t

```
enum hsm_err_t
```

Error codes returned by HSM functions.

## Enumerator

HSM_NO_ERROR	Success.
HSM_OUT_OF_MEM	There is not enough memory to open a new session or service flow.
HSM_UNKNOWN_HANDLE	The provided handle doesn't exist
HSM_UNKNOWN_KEY_STORE	The provided key store identifier doesn't exist
HSM_KEY_STORE_AUTH_ERROR	Key store authentication fails
HSM_UNKNOWN_ID	The provided identifier doesn't exist.
HSM_BUF_SIZE_ERROR	The size of the buffer provided by the requester is too small for the requested operation
HSM_KEY_ERROR	The key cannot be used for the requested operation.
HSM_MEM_ACCESS_ERROR	The specified memory address cannot be accessed.
HSM_INVALID_PARAM	One or more parameters are not valid
HSM_GENERAL_ERROR	Error not covered by other codes occurred.

#### 4.1.4 Function Documentation

##### 4.1.4.1 hsm\_open\_session()

```
struct hsm_hdl_s* hsm_open_session (
    uint32_t key_storage_identifier,
    uint8_t access_flags,
    uint32_t password,
    uint8_t session_priority,
    uint8_t operating_mode )
```

Initiate a HSM session granting the usage of the specified key store.

The returned handle pointer is typed with the transparent struct "hsm\_hdl\_s". The user doesn't need to know or to access the fields of this struct. They only need to store this pointer and pass it to every calls to other APIs within the same HSM session.

##### Parameters

<i>key_storage_identifier</i>	key store identifier
<i>access_flags</i>	bitmap indicating the requested access to the key store. The create flag must be specified to create a new key storage.
<i>password</i>	password for accesing the key storage
<i>session_priority</i>	not supported in current release, any value accepted.
<i>operating_mode</i>	not supported in current release, any value accepted.

##### Returns

pointer to the HSM handle.

##### 4.1.4.2 hsm\_close\_session()

```
hsm_err_t hsm_close_session (
    struct hsm_hdl_s * hdl )
```

Terminate a previously opened HSM session

##### Parameters

<i>hdl</i>	pointer to the HSM handle to be closed.
------------	---

##### Returns

error code

#### 4.1.4.3 hsm\_open\_key\_management\_service()

```
hsm_err_t hsm_open_key_management_service (
    struct hsm_hdl_s * hdl,
    uint32_t input_address_ext,
    uint32_t output_address_ext )
```

Open a key management service flow

User must open this service in order to perform operation on the keys (generate, delete, update)

##### Parameters

<i>hdl</i>	pointer to the HSM handle
<i>input_address_ext</i>	most significant 32 bits address to be used by HSM for input memory transactions in the requester address space for the commands handled by the service flow.
<i>output_address_ext</i>	most significant 32 bits address to be used by HSM for output memory transactions in the requester address space for the commands handled by the service flow.

##### Returns

error code

#### 4.1.4.4 hsm\_key\_management\_cmd\_key\_generation()

```
hsm_err_t hsm_key_management_cmd_key_generation (
    struct hsm_hdl_s * hdl,
    uint8_t * key_identifier,
    uint8_t * output,
    uint16_t key_type,
    uint8_t output_size,
    uint8_t flags )
```

Generate a key or a key pair in the key store. The public key can optionally be exported

User can call this function only after having opened a key management service flow

##### Parameters

<i>hdl</i>	pointer to the HSM handle
<i>key_identifier</i>	pointer to the identifier of the key slot to be used for the operation - The value HSM_KEY_IDENTIFIER_NEW indicates to create a new key slot
<i>output</i>	pointer to the output area to store the public key - A NULL pointer indicates to not store the public key
<i>key_type</i>	indicates which type of key must be generated
<i>output_size</i>	length in bytes of the output area
<i>flags</i>	bitmap specifying the properties of the key

##### Returns

error code



#### 4.1.4.5 hsm\_close\_key\_management\_service()

```
hsm_err_t hsm_close_key_management_service (
    struct hsm_hdl_s * hdl )
```

Terminate a previously opened key management service flow

##### Parameters

<i>hdl</i>	pointer to the HSM handle.
------------	----------------------------

##### Returns

error code

#### 4.1.4.6 hsm\_open\_cipher\_service()

```
hsm_err_t hsm_open_cipher_service (
    struct hsm_hdl_s * hdl,
    uint32_t input_address_ext,
    uint32_t output_address_ext,
    uint8_t flags )
```

Open a cipher service flow

User must open this service in order to perform cipher operations.

##### Parameters

<i>hdl</i>	pointer to the HSM handle
<i>input_address_ext</i>	most significant 32 bits address to be used by HSM for input memory transactions in the requester address space for the operations handled by the service flow.
<i>output_address_ext</i>	most significant 32 bits address to be used by HSM for output memory transactions in the requester address space for the operation handled by the service flow.
<i>flags</i>	bitmap indicating the service flow properties - not supported in current release, any value accepted.

##### Returns

error code

#### 4.1.4.7 hsm\_cipher\_cmd\_cipher\_one\_go()

```
hsm_err_t hsm_cipher_cmd_cipher_one_go (
    struct hsm_hdl_s * hdl,
    uint32_t key_identifier,
    uint8_t * input,
    uint8_t * output,
```

```
uint8_t * iv,  
uint32_t * input_size,  
uint16_t iv_size,  
uint8_t algorithm,  
uint8_t flags )
```

Prperform ciphering operation

User can call this function only after having opened a cipher service flow

#### Parameters

<i>hdl</i>	pointer to the HSM handle
<i>key_identifier</i>	identifier of the key to be used for the operation
<i>input</i>	pointer to the input to be processed
<i>output</i>	pointer to the output area
<i>iv</i>	pointer to the initialization vector - it must be NULL for algorithms not using the initialization vector
<i>input_size</i>	length in bytes of the input
<i>iv_size</i>	length in bytes of the initialization vector - it must be 0 for algorithms not using the initialization vector
<i>algorithm</i>	to be used for the operation
<i>flags</i>	bitmap specifying the operation attributes

#### Returns

error code

#### 4.1.4.8 hsm\_close\_cipher\_service()

```
hsm_err_t hsm_close_cipher_service (  
    struct hsm_hdl_s * hdl )
```

Terminate a previously opened cipher service flow

#### Parameters

<i>hdl</i>	pointer to the HSM handle.
------------	----------------------------

#### Returns

error code



## Index

Hsm\_api, 1  
HSM\_BUF\_SIZE\_ERROR, 5  
hsm\_cipher\_cmd\_cipher\_one\_go, 8  
HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_CBC, 5  
HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_ECB, 4  
HSM\_CIPHER\_ONE\_GO\_FLAGS\_DECRYPT, 5  
HSM\_CIPHER\_ONE\_GO\_FLAGS\_ENCRYPT, 5  
hsm\_close\_cipher\_service, 9  
hsm\_close\_key\_management\_service, 7  
hsm\_close\_session, 6  
hsm\_err\_t, 5  
HSM\_GENERAL\_ERROR, 5  
HSM\_INVALID\_PARAM, 5  
HSM\_KEY\_ERROR, 5  
HSM\_KEY\_FLAGS\_PERMANENT, 4  
HSM\_KEY\_FLAGS\_TRANSIENT, 4  
HSM\_KEY\_IDENTIFIER\_NEW, 3  
hsm\_key\_management\_cmd\_key\_generation, 7  
HSM\_KEY\_STORAGE\_ACCESS\_FLAG\_NEW, 3  
HSM\_KEY\_STORE\_AUTH\_ERROR, 5  
HSM\_KEY\_TYPE\_AES\_128, 4  
HSM\_KEY\_TYPE\_AES\_192, 4  
HSM\_KEY\_TYPE\_AES\_256, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_224, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_256, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_384, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_224, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_256, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_384, 4  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P224, 3  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P256, 3  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P384, 3  
HSM\_MEM\_ACCESS\_ERROR, 5  
HSM\_NO\_ERROR, 5  
hsm\_open\_cipher\_service, 8  
hsm\_open\_key\_management\_service, 6  
hsm\_open\_session, 6  
HSM\_OUT\_OF\_MEM, 5  
HSM\_UNKNOWN\_HANDLE, 5  
HSM\_UNKNOWN\_ID, 5  
HSM\_UNKNOWN\_KEY\_STORE, 5  
HSM\_BUF\_SIZE\_ERROR  
Hsm\_api, 5  
hsm\_cipher\_cmd\_cipher\_one\_go  
Hsm\_api, 8  
HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_CBC  
Hsm\_api, 5  
HSM\_CIPHER\_ONE\_GO\_ALGO\_AES\_ECB  
Hsm\_api, 4  
HSM\_CIPHER\_ONE\_GO\_FLAGS\_DECRYPT  
Hsm\_api, 5  
HSM\_CIPHER\_ONE\_GO\_FLAGS\_ENCRYPT  
Hsm\_api, 5  
hsm\_close\_cipher\_service  
Hsm\_api, 9  
hsm\_close\_key\_management\_service  
Hsm\_api, 7  
hsm\_close\_session  
Hsm\_api, 6  
hsm\_err\_t  
Hsm\_api, 5  
HSM\_GENERAL\_ERROR  
Hsm\_api, 5  
HSM\_INVALID\_PARAM  
Hsm\_api, 5  
HSM\_KEY\_ERROR  
Hsm\_api, 5  
HSM\_KEY\_FLAGS\_PERMANENT  
Hsm\_api, 4  
HSM\_KEY\_FLAGS\_TRANSIENT  
Hsm\_api, 4  
HSM\_KEY\_IDENTIFIER\_NEW  
Hsm\_api, 3  
hsm\_key\_management\_cmd\_key\_generation  
Hsm\_api, 7  
HSM\_KEY\_STORAGE\_ACCESS\_FLAG\_NEW  
Hsm\_api, 3  
HSM\_KEY\_STORE\_AUTH\_ERROR  
Hsm\_api, 5  
HSM\_KEY\_TYPE\_AES\_128  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_AES\_192  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_AES\_256  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_224  
Hsm\_api, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_256  
Hsm\_api, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_R1\_384  
Hsm\_api, 3  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_224  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_256  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_ECDSA\_BRAINPOOL\_T1\_384  
Hsm\_api, 4  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P224  
Hsm\_api, 3  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P256  
Hsm\_api, 3  
HSM\_KEY\_TYPE\_ECDSA\_NIST\_P384  
Hsm\_api, 3  
HSM\_MEM\_ACCESS\_ERROR

Hsm\_api, [5](#)  
HSM\_NO\_ERROR  
Hsm\_api, [5](#)  
hsm\_open\_cipher\_service  
Hsm\_api, [8](#)  
hsm\_open\_key\_management\_service  
Hsm\_api, [6](#)  
hsm\_open\_session  
Hsm\_api, [6](#)  
HSM\_OUT\_OF\_MEM  
Hsm\_api, [5](#)  
HSM\_UNKNOWN\_HANDLE  
Hsm\_api, [5](#)  
HSM\_UNKNOWN\_ID  
Hsm\_api, [5](#)  
HSM\_UNKNOWN\_KEY\_STORE  
Hsm\_api, [5](#)