MUSCLECARD FRAMEWORK
Application Programming Interface

The MUSCLE Group
version 1.3.0

This document is provided on an AS-IS basis. Neither the authors nor members of the MUSCLE group are responsible for any mishaps, misuse, or loss caused by the use of this document and specification. This

This document describes the client side API fo

v k a h y l n o m m o c

MUSCLECARD FUNCTIONS

Function Name	Function Description
MSCListTokens	- List tokens available
MSCEstablishConnection	- Connects to a token
MSCReleaseConnection	- Releases a token

MSCTokenConnection, *MSCLPTokenConnection

- This structure is used as a handle to all functions after a connection is made to a token.

[

MSCUChar8	*pMac*	- MAC cryptogram used for secure comm (RFU)
MSCULong32	*macSize*	- Size of the cryptogram
MSCTokenInfo	tokenInfo	- Token information for a particular connection

]

MSCStatusInfo, *MSCLPStatusInfo

- This structure is returned from MSCGetStatus which contains status information about the token. Capability information should be requested using MSCGetCapabilities.

MSCKeyPolicy, *MSCLPKeyPolicy

- This structure is used to both describe a key usage policy for a key.

[

MSCUShort16 *cipherMode* - Bitmask of usage modes for policy

[

NAME

MSCListTokens – Lists tokens available on the system

[redacted]

NAME

MSCWaitForTokenEvent – Waits for a token event

SYNOPSIS

```
#include <musclecard.h>

MSCWaitForTokenEvent(
  MSCLPTokenInfo      tokenArray,
  MSCULong32          arraySize,
  MSCULong32          timeoutValue
);
```

PARAMETERS

tokenArray	Array of token structures
arraySize	Number of token structure in array
timeoutValue	Timeout value in milliseconds

DESCRIPTION

This function waits (blocks) for an event to occur on a particular token or tokens.   The application may either specify which events it is interested in or it may choose to block for any event. Typical events would include the insertion or removal of a token into a particular slot. A newly inserted token would update the friendlyname of the token if it

```
pParams.privateKeyPolicy
pParams.publicKeyPolicy

  pParams.privateKeyPolicy.cipherDirection
  pParams.publicKeyPolicy.cipherDirection
    MSC_KEYPOLICY_DIR_SIGN            Can be used for signing
    MSC_KEYPOLICY_DIR_VERIFY          Can be used for verification
    MSC_KEYPOLICY_DIR_ENCRYPT         Can be used for encryption
    MSC_KEYPOLICY_DIR_DECRYPT         Can be used for decryption

  pParams.privateKeyPolicy.cipherMode
  pParams.publicKeyPolicy.cipherMode
    MSC_KEYPOLICY_MODE_RSA_NOPAD      RSA can be used with no pad
    MSC_KEYPOLICY_MODE_RSA_PAD_PKCS1  RSA can be used with pkcs pad
    MSC_KEYPOLICY_MODE_DSA_SHA        DSA can be used with SHA
    MSC_KEYPOLICY_MODE_DES_CBC_NOPAD  DES can be used CBC nopad
    MSC_KEYPOLICY_MODE_DES_ECBPAD  DES can be used CBCECB nopad

pParams.keyGenOptions
  MSC_OPT_DEFAULT                     Use default options

pParams.pOptParams
 Reserved for futursed C (RFU)

pParams.optParamsSize
 Reserved for futursed C (RFU)
```

RETURN H1.796A78 T57 TD 0 Tc ( )H1.RD ( )TjTj /F2 1 Tf 0 -1.1078eferMSCe previouslyTJ Tin()

NAME

MSCExtAuthenticate - Authenticate the host to the card.

SYNOPSIS

```
#include <musclecard.h>

MSCExtAuthenticate(
  MSCLPTokenConnection      pConnection,
  MSCUChar8                 keyNum,
  MSCUChar8                 cipherMode,
  MSCUChar8                 cipherDirection,
  MSCPUChar8                pData,
  MSCULong32                dataSize
);
```

PARAMETERS

pConnection	Handle to a previously connected session
keyNum	Key number for operation
cipherMode	Cipher mode to use
cipherDirection	Direction of the cipher
pData	Data presented to the card
dataSize	Size of pData

DESCRIPTION

This function authenticates the host to the card. When the host calls a GetChallenge it can present this value back to the card ciphered with a particular key. The card will use an internal key to decipher the data presented to the card andj Ttermine whether the host is validated.

cipherMode

MSC_MODE_RSA_NO_PAD	Use RSA andj on't pad
MSC_MODE_DSA_SHA	Use DSA with SHA
MSC_MODE_DES_CBC_NOPAD	Use DES in CBC mode
MSC_MODE_DES_ECB_NOPAD	Use DES in ECB mode

cipherDirection

MSC_DIR_SIGN	Perform a signing operation
MSC_DIR_VERIFY	Verify a signature
MSC_DIR_ENCRYPT	Encrypt the data
MSC_DIR_DECRYPT	Decrypt the data

RETURN VALUES

Reference previously defined error codes.

EXAMPLES

```
MSCTokenInfo tokenList[16];  // 16 used as example
MSCTokenConnection pConnection;
MSCCryptInit myCrypt;
MSCUChar8 seedData[20], randomData[20];
MSCUChar8 cipherData[20];
MSCULong32 outSize;
MSC_RV rv; MSCULong32 listSize = 16;

rv = MSCListTokens( MSC_LIST_KNOWN, tokenList, &listSize );
if (rv == MSC_SUCCESS) {
```

NAME

MSCListKeys - Lists the currently available keys

NAME

MSCGetChallenge - Retrieve a random number from the card

SYNOPSIS

```
#include <munclecard.h>
 MSCGetChallenge(     MSCLPTokenConnection      pConnection,
  MSCPUChar8                pSeed,     MSCUShort16               seedSize,     MSCPUChar8
```

PARAMETERS

```
pConnection           Handle to a previously connected session
pSeed                 Seed to inject into random algorithm   seedSize              Size o
randomDataSize        Amount of random data requested
```

DESCRIPTION

This function requests a random number from the card which can be used for many purposes including the verify an authentication   using the MSCExtAuthen into pSeed. A seedSize of zero denotes no seed presented.

RETURN VALUES

Reference previously defined error codes.

EXAMPLES

```
MSCTokenInfo tokenList[16];  // 16 used as example   MSCTokenConnection pConnect
```

SEE ALSO

MSC_TAG_CAPABLE_PIN_MINSIZE [1]

This tag returns the minimum number of characters which may be used in a pin. For example, a return of 4 means you may have a minimum pin size of 4 characters.

MSC_TAG_CAPABLE_PIN_MAXSIZE [1]

This tag returns the maximum number of characters which may be used in a pin. For example, a return of 8 means you may have a maximum pin size of 8 characters.

MSC_TAG_CAPABLE_PIN_CHARSET [4]

This Tag returns a bitmask of the supported character set based on the pin policy set in the token:

MSC_CAPABLE_PIN_A_Z	-Supports uppercase A-Z
MSC_CAPABLE_PIN_a_z	-Supports lowercase a-z
MSC_CAPABLE_PIN_0_9	-Supports numbers 0-9

MSC_CA