

Product Name	Confidentiality level
mToken CryptoID	
Product version	
V3.0	

mToken CryptoID PKCS11 Guide



Century Longmai Technology Co., Ltd.

All rights reserved

Revision Record

Date	Revision Version	Sec No.	Change Description	Author
2016/12/04	V1.0		Initial Version	Longmai ITD

Table of Contents

1. INTRODUCTION 3

2. SUPPORTED MECHANISMS 3

3. SUPPORTED FUNCTIONS 4

4. ABOUT CENTURY LONGMAI..... 7

CENTURY LONGMAI TECHNOLOGY CO., LTD..... 7

1. Introduction

The mToken CryptoID provide PKCS11 for application integration, it's compliant with the PKCS11 V2.20 standard and support Windows, Linux and Mac OS.

Please refer to the pkcs11 standard document for more details.

2. Supported Mechanisms

Algorithm	Encrypt/ Decrypt	Sign/ Verify	Digest	Key Gen	Wrap
CKM_RSA_PKCS_KEY_PAIR_GEN				√	
CKM_RSA_PKCS	√	√			√
CKM_RSA_X_509	√	√			
CKM_RSA_X9_31_KEY_PAIR_GEN				√	
CKM_RSA_X9_31		√			
CKM_SHA1_RSA_X9_31		√			
CKM_SHA1_RSA_PKCS		√			
CKM_SHA256_RSA_PKCS		√			
CKM_SHA384_RSA_PKCS		√			
CKM_SHA512_RSA_PKCS		√			
CKM_MD5_RSA_PKCS		√			
CKM_RC2_KEY_GEN				√	
CKM_RC2_ECB	√				
CKM_RC2_CBC	√				
CKM_RC4_KEY_GEN				√	
CKM_RC4	√				
CKM_DES_KEY_GEN				√	
CKM_DES_ECB	√				√
CKM_DES_CBC	√				√
CKM_DES_CBC_PAD	√				√
CKM_DES3_KEY_GEN				√	
CKM_DES3_ECB	√				√
CKM_DES3_CBC	√				√
CKM_DES3_CBC_PAD	√				√

CKM_AES_KEY_GEN	√				
CKM_AES_ECB	√				
CKM_AES_CBC	√				
CKM_AES_CBC_PAD	√				
CKM_MD5			√		
CKM_SHA_1			√		
CKM_SHA256			√		
CKM_SHA512			√		
CKM_MD5_KEY_DERIVATION				√	
CKM_SHA1_KEY_DERIVATION				√	
CKM_SHA256_KEY_DERIVATION				√	
CKM_SHA512_KEY_DERIVATION				√	
CKM_MD5_HMAC			√		
CKM_SHA1_HMAC			√		
CKM_SHA256_HMAC			√		
CKM_SHA512_HMAC			√		

3. Supported Functions

Function Name	Implemented or Not
C_Initialize,	Implemented
C_Finalize,	Implemented
C_GetInfo,	Implemented
C_GetFunctionList,	Implemented
C_GetSlotList,	Implemented
C_GetSlotInfo,	Implemented
C_GetTokenInfo,	Implemented
C_GetMechanismList,	Implemented
C_GetMechanismInfo,	Implemented
C_InitToken,	Implemented
C_InitPIN,	Implemented
C_SetPIN,	Implemented
C_OpenSession,	Implemented
C_CloseSession,	Implemented
C_CloseAllSessions,	Implemented
C_GetSessionInfo,	Implemented

C_GetOperationState,	Not Implemented
C_SetOperationState,	Not Implemented
C_Login,	Implemented
C_Logout,	Implemented
C_CreateObject,	Implemented
C_CopyObject,	Implemented
C_DestroyObject,	Implemented
C_GetObjectSize,	Implemented
C_GetAttributeValue,	Implemented
C_SetAttributeValue,	Implemented
C_FindObjectsInit,	Implemented
C_FindObjects,	Implemented
C_FindObjectsFinal,	Implemented
C_EncryptInit,	Implemented
C_Encrypt,	Implemented
C_EncryptUpdate,	Implemented
C_EncryptFinal,	Implemented
C_DecryptInit,	Implemented
C_Decrypt,	Implemented
C_DecryptUpdate,	Implemented
C_DecryptFinal,	Implemented
C_DigestInit,	Implemented
C_Digest,	Implemented
C_DigestUpdate,	Implemented
C_DigestKey,	Implemented
C_DigestFinal,	Implemented
C_SignInit,	Implemented
C_Sign,	Implemented
C_SignUpdate,	Implemented
C_SignFinal,	Implemented
C_SignRecoverInit,	Not Implemented
C_SignRecover,	Not Implemented
C_VerifyInit,	Implemented
C_Verify,	Implemented
C_VerifyUpdate,	Implemented
C_VerifyFinal,	Implemented
C_VerifyRecoverInit,	Not Implemented
C_VerifyRecover,	Not Implemented

C_DigestEncryptUpdate,	Implemented
C_DecryptDigestUpdate,	Implemented
C_SignEncryptUpdate,	Implemented
C_DecryptVerifyUpdate,	Implemented
C_GenerateKey,	Implemented
C_GenerateKeyPair,	Implemented
C_WrapKey,	Implemented
C_UnwrapKey,	Implemented
C_DeriveKey,	Implemented
C_SeedRandom,	Implemented
C_GenerateRandom,	Implemented
C_GetFunctionStatus,	Not Implemented
C_CancelFunction,	Not Implemented
C_WaitForSlotEvent,	Implemented

4. About Century Longmai

Established in 2003, Century Longmai Technology Co., Ltd is one of the most leading information security device vendors in China with over 12 years' experience developing latest generation of digital security solutions and products for secure information access and transmission. Our product portfolios include PKI dongles, wireless PKI tokens, OTP tokens, smart card, smart card readers, electronic document protection solution, software license dongles, Smartcard readers and OEM services. Proved to be secure and convenient, our solutions and products are dedicated to help customers build safe, efficient and sustainable networks, financial systems and enjoy secure access to data and information everywhere whenever they want.

Century Longmai Technology Co., Ltd

3rd Floor, GongKong Building, No.1, WangZhuang Road, Haidian District, Beijing, China

Postcode: 100083

Tel: (86) 10-62323636 | Fax: (86) 10-62313636

Sales E-mail: info@longmai.net Support E-mail: support@longmai.net

Website: <http://www.longmai.net>