VIRBOX

密码学算法 API 参考

Version 1.0.0.0

许可协议

同意本许可协议的所有条款及此处包含的任何补充或特殊的许可条款是获得本产品许可的必要条件。如果您不同意此协议的所有条款，请在三天内将产品退还北京深思数盾科技股份有限公司。您对本软件的使用将表明您同意接受本协议中条款的约束。

1. 授予您使用许可权。您可以为了备份的目的而复制磁盘中的软件，可以为了将本产品集成到您的软件的目的，根据本产品的文档说明将我们提供的软件合并进您的程序中。
2. 除已按上述第一条被授权外，不可以复制、修改、逆向工程、分解或重组该产品的全部或部分，不可向他人销售、租借、许可、转让、分发全部或部分本产品或本协议授予的权利。
3. 保证在自产品交给您之日起的 12 个月内，在正常使用情况下，产品不会出现实质性的材料上和生产制造上的缺陷。北京深思数盾科技股份有限公司的全部责任和您能获得的全部补救措施为：可选择尝试更换或修理或其他补救措施。
4. 除了上述对本产品的原始购买者所提供的有限保证之外，不向任何人作任何其他的保证。对北京深思数盾科技股份有限公司的产品、性能或服务亦没有明示的或暗示的或其他任何形式的保证，包括但不仅仅限于商品的适销性和对特定用途的适用性。
5. 任何情况下，无论如何引起及依据何种责任理论，均不负担任何因使用或不能使用本产品造成的损失责任，包括：丢失数据、损失利润及其他特别的、偶然的、附随的、继发的或间接的损失。
6. 所有的产品，包括魔锐设备、软件、文档、与本产品一并附送的其他材料及您制作的备份的所有权与版权均属于北京深思数盾科技股份有限公司。
7. 违反上述条款时，本协议的授权将自动终止。

联系深思数盾

公司名称：北京深思数盾科技股份有限公司
办公地点：北京市海淀区西北旺东路 10 号院 5 号楼软件园二期互联网创新中心 C510
邮　　编：100872
电　　话：+86-10-556730936
传　　真：+86-10-556730936
电子邮件：sense@sense.com.cn
网　　址：http://www.sense.com.cn

阅读指南

〖手册目标〗

本手册主要对北京深思数盾科技股份有限公司开发的魔锐加密锁的使用进行说明，由于实际情况千变万化，本手册很难一次做到面面俱到，需要逐渐完善。

〖手册约定〗

手册中出现该标志的地方表示需要您引起高度重视，否则可能会引发严重的后果。

手册中出现该标志的地方表示需要您特别引起注意的内容。

目 录

第1章 常量说明

1.1 密钥类型 ID

序号	宏名	数值	说明
1	SLC_KEY_SYMMETRIC	0x01	密钥属于对称加密算法。包括：AES，TDES，DES。
2	SLC_KEY_PUBLIC	0x02	密钥属于公开密钥算法的公钥。包括：RSA、ECC 算法的公钥。
3	SLC_KEY_PRIVATE	0x03	密钥属于公开密钥算法的私钥。包括：RSA、ECC 算法的私钥。
4	SLC_KEY_HMAC	0x04	密钥属于 HMAC 计算的密钥。包括：MD5、SHA1、SHA256。

说明：SLC_KEY 类型密钥的类型代号。用于 SlcCheckKeyType 函数。

1.2 加密算法 ID

序号	宏名	数值	说明
1	SLC_CIPHER_ALGO_AES	0x00	密钥用于 AES 算法。
2	SLC_CIPHER_ALGO_DES	0x01	密钥用于 DES 算法。
3	SLC_CIPHER_ALGO_TDES	0x02	密钥用于 TDES 算法。
4	SLC_CIPHER_ALGO_ECC	0x10	密钥用于 ECC 算法。
5	SLC_CIPHER_ALGO_RSA	0x11	密钥用于 RSA 算法。
6	SLC_CIPHER_ALGO_HMAC_MD5	0x41	密钥用于 HMAC-MD5 计算
7	SLC_CIPHER_ALGO_HMAC_SHA1	0x42	密钥用于 HMAC-SHA1 计算
8	SLC_CIPHER_ALGO_HMAC_SHA256	0x43	密钥用于 HMAC-SHA256 计算

说明：SLC_KEY 类型密钥的算法代号。用于 SlcCheckKeyType 函数。

1.3 DES/TDES/AES 算法的加密模式 ID

序号	宏名	数值	说明
1	SLC_MODE_ECB	0x00	对称算法 ECB 模式
2	SLC_MODE_CBC	0x01	对称算法 CBC 模式

1.4 HASH 算法 ID

序号	宏名	数值	说明
1	SLC_HASH_ALGO_SHA1	0x01	SHA1 哈希摘要算法
2	SLC_HASH_ALGO_SHA256	0x02	SHA256 哈希摘要算法
3	SLC_HASH_ALGO_MD5	0x03	MD5 哈希摘要算法

1.5 RSA 算法中的填充模式 ID

序号	宏名	数值	说明
1	SLC_PAD_MODE_NONE	0x00	RSA 算法不需要填充
2	SLC_PAD_MODE_PKCS_1_V1_5	0x01	RSA 算法使用 PKCS1 模式填充

1.6 密钥长度定义

序号	宏名	数值	说明
1	SLC_DES_KEY_BIT_LEN	56	DES 算法密钥长度
2	SLC_TDES_KEY_BIT_LEN	112	TDES 算法密钥长度
3	SLC_AES_KEY_BIT_128	128	AES 算法密钥长度为 128 位
4	SLC_AES_KEY_BIT_192	192	AES 算法密钥长度为 192 位
5	SLC_AES_KEY_BIT_256	256	AES 算法密钥长度为 256 位
6	SLC_RSA_KEY_BIT_1024	1024	RSA 算法密钥长度为 1024 位
7	SLC_RSA_KEY_BIT_2048	2048	RSA 算法密钥长度为 2048 位
8	SLC_RSA_KEY_BIT_4096	4096	RSA 算法密钥长度为 4096 位
9	SLC_ECC_KEY_BIT_192	192	ECC 算法密钥长度为 192 位
10	SLC_ECC_KEY_BIT_256	256	ECC 算法密钥长度为 256 位

1.7 DES/TDES/AES 加密算法的数据块长度

序号	宏名	数值	说明
1	SLC_DES_BLOCK_SIZE	8	对称算法 DES 分组字节长度
2	SLC_TDES_BLOCK_SIZE	8	对称算法 TDES 分组字节长度
3	SLC_AES_BLOCK_SIZE	16	对称算法 AES 分组字节长度

1.8 HASH 算法的摘要长度（字节数）

序号	宏名	数值	说明
1	SLC_MD5_DIGEST_LEN	16	MD5 摘要字节长度
2	SLC_SHA1_DIGEST_LEN	20	SHA1 摘要字节长度
3	SLC_SHA256_DIGEST_LEN	32	SHA256 摘要字节长度

1.9 签名算法的签名长度（字节数）

序号	宏名	数值	说明
1	SLC_RSA1024_SIG_LEN	128	RSA1024 算法签名字节长度
2	SLC_RSA2048_SIG_LEN	256	RSA2048 算法签名字节长度
3	SLC_RSA4096_SIG_LEN	512	RSA4096 算法签名字节长度
4	SLC_ECC192_SIG_MAX_LEN	128	ECC192 算法签名字节长度
5	SLC_ECC256_SIG_MAX_LEN		ECC256 算法签名字节长度

第2章 返回值

序号	返回值宏名	数值	说明
1	SLC_SUCCESS	0x0000	执行成功
2	SLC_ERROR_NO_MEMORY	0x0001	分配内存失败
3	SLC_ERROR_INVALID_PARAMETER	0x0002	无效参数(一般是指使用了 NULL 指针)
4	SLC_ERROR_INVALID_HASH_ALGO	0x0003	无效的 HASH 算法 ID

序号	返回值宏名	数值	说明
5	SLC_ERROR_INVALID_CIPHER_ALGO	0x0004	无效的加密算法 ID
6	SLC_ERROR_INVALID_MODE	0x0005	无效的加密模式或填充模式
7	SLC_ERROR_INPUTDATA_LENGTH	0x0006	输入数据的长度错误
8	SLC_ERROR_INSUFFICIENT_BUFFER	0x0007	输出缓冲区的长度不足
9	SLC_ERROR_INVALID_KEY_SIZE	0x0008	密钥长度错误
10	SLC_ERROR_MAKE_KEY	0x0009	生成密钥失败
11	SLC_ERROR_SIGN	0x000A	签名失败
12	SLC_ERROR_VERIFY	0x000B	验证签名失败（数据与签名不匹配）
13	SLC_ERROR_INVALID_INPUT_DATA	0x000C	无效的输入数据
14	SLC_ERROR_BAD_KEY_FORMAT	0x000D	密钥格式错误
15	SLC_ERROR_BAD_KEY_VERSION	0x000E	密钥版本错误
16	SLC_ERROR_BAD_KEY_ALGORITHM	0x000F	密钥算法错误
17	SLC_ERROR_BAD_KEY_TYPE	0x0010	密钥类型错误
18	SLC_ERROR_BAD_PADDING	0x0011	填充格式错误
19	SLC_ERROR_UNKNOW	0x0012	未预期的错误（API 内部错误。应该不会出现）

第3章 类型定义

```
#ifndef SLC_BYTE
typedef unsigned char      SLC_BYTE;
#endif

#ifndef SLC_ULONG
typedef unsigned long      SLC_ULONG;
#endif

typedef void *             SLC_HASH_CTX;
typedef void *             SLC_KEY;
```

第4章 函数说明

4.1 SlcAesEncRaw

AES 加密函数。使用 16，24，32 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcAesEncRaw(
                    IN      SLC_BYTE            byMode,
                    IN      const SLC_BYTE      * pbKey,
                    IN      SLC_ULONG           ulKeyBitLen,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf,
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	AES 密钥缓冲区。可为 16，24，32 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulKeyBitLen	密钥位数。可取值 128，192，256，分别对应 16，24，32 字节的密钥。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 16 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH

pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.2 SlcAesDecRaw

AES 解密函数。使用 16，24，32 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcAesDecRaw(
                    IN      SLC_BYTE            byMode,
                    IN      const SLC_BYTE      * pbKey,
                    IN      SLC_ULONG           ulKeyBitLen,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB，SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	AES 密钥缓冲区。可为 16，24，32 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulKeyBitLen	密钥位数。可取值 128，192，256，分别对应 16，24，32 字节的密钥。

	出错返回值：SLC_ERROR_INVALID_KEY_SIZE
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 16 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.3 SlcAesGenerateKey

生成 SLC_KEY 格式的 AES 密钥。
如果有以前使用的无格式密钥，则可用以前的无格式密钥对所生成的 SLC_KEY 格式的密钥做初始化，使 SLC_KEY 密钥包含原来的无格式密钥。

```
SLC_ULONG SLCAPI SlcAesGenerateKey(
                        IN      const SLC_BYTE          * pbInitData,
                        IN      SLC_ULONG               ulKeyBitLen,
                        OUT     SLC_KEY                 * pSlcKey
                        );
```

参数说明：

pbInitData	以前的使用的无格式密钥。可为 16，24，32 字节。可以为 NULL。 如果取值为 NULL，则此函数将生成随机数作为密钥。
ulKeyBitLen	密钥位数。可取值 128，192，256。 取值 128（SLC_AES_KEY_BIT_128），对应 16 字节的密钥。 取值 192（SLC_AES_KEY_BIT_192），对应 24 字节的密钥。 取值 256（SLC_AES_KEY_BIT_256），对应 32 字节的密钥。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE.
pSlcKey	传入一个 SLC_KEY 变量的地址。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.4 SlcAesEnc

AES 加密函数。使用 SLC_KEY 格式的 AES 密钥。

```
SLC_ULONG SLCAPI SlcAesEnc(
                    IN      SLC_BYTE            byMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。

SlcKey	SLC_KEY 格式的 AES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 16 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.5 SlcAesDec

AES 解密函数。使用 SLC_KEY 格式的 AES 密钥。

```
SLC_ULONG SLCAPI SlcAesDec(
                        IN      SLC_BYTE                byMode,
                        IN      SLC_KEY             SlcKey,
```

```
IN      const SLC_BYTE          * pbIv,
IN      const SLC_BYTE          * pbData,
IN      SLC_ULONG               ulDataLen,
OUT     SLC_BYTE                * pbOutBuf
IN      SLC_ULONG               ulOutBufLen,
OUT     SLC_ULONG               * pulOutDataLen
);
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
SlcKey	SLC_KEY 格式的 AES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 16 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.6 SlcDesEncRaw

DES 加密函数。使用 8 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcDesEncRaw(
                    IN      SLC_BYTE            byMode,
                    IN      const SLC_BYTE      * pbKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	DES 密钥缓冲区。8 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。

	出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.7 SlcDesDecRaw

DES 加密函数。使用 8 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcDesDecRaw(
                    IN      SLC_BYTE            byMode,
                    IN      const SLC_BYTE      * pbKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	DES 密钥缓冲区。8 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向

	量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.8 SlcDesGenerateKey

生成 SLC_KEY 格式的 DES 密钥。
如果有以前使用的无格式密钥，则可用以前的无格式密钥对所生成的 SLC_KEY 格式的密钥做初始化，使 SLC_KEY 密钥包含原来的无格式密钥。

```
SLC_ULONG SLCAPI SlcDesGenerateKey(
                    IN      const SLC_BYTE          * pbInitData,
                    IN      SLC_ULONG               ulKeyBitLen,
                    OUT     SLC_KEY                 * pSlcKey
                    );
```

参数说明：

pbInitData	以前的使用的无格式密钥。8 字节。可以为 NULL。 如果取值为 NULL，则此函数将生成随机数作为密钥。
ulKeyBitLen	密钥位数。可取值 56(SLC_DES_KEY_BIT_LEN)。

	出错返回值：SLC_ERROR_INVALID_KEY_SIZE.
pSlcKey	传入一个 SLC_KEY 变量的地址。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.9 SlcDesEnc

DES 加密函数。使用 SLC_KEY 无格式的 DES 密钥。

```
SLC_ULONG SLCAPI SlcDesEnc(
                    IN      SLC_BYTE            byMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
SlcKey	SLC_KEY 格式的 DES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向

	量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.10 SlcDesDec

DES 加密函数。使用 SLC_KEY 格式的 DES 密钥。

```
SLC_ULONG SLCAPI SlcDesDec(
                    IN      SLC_BYTE            byMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC.

	出错返回值：SLC_ERROR_INVALID_MODE。
SlcKey	SLC_KEY 格式的 DES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.11 SlcTDesEncRaw

TDES 加密函数。使用 16 字节的无格式密钥。

SLC_ULONG SLCAPI SlcTDesEncRaw(

```
IN      SLC_BYTE                byMode,
IN      const SLC_BYTE          * pbKey,
IN      const SLC_BYTE          * pbIv,
IN      const SLC_BYTE          * pbData,
IN      SLC_ULONG               ulDataLen,
OUT     SLC_BYTE                * pbOutBuf
IN      SLC_ULONG               ulOutBufLen,
OUT     SLC_ULONG               * pulOutDataLen
);
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	TDES 密钥缓冲区。16 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：

成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.12 SlcTDesDecRaw

TDES 加密函数。使用 16 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcTDesDecRaw(
                    IN      SLC_BYTE            byMode,
                    IN      const SLC_BYTE      * pbKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	AES 密钥缓冲区。16 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。

ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.13 SlcTDesGenerateKey

生成 SLC_KEY 格式的 TDES 密钥。
如果有以前使用的无格式密钥，则可用以前的无格式密钥对所生成的 SLC_KEY 格式的密钥做初始化，使 SLC_KEY 密钥包含原来的无格式密钥。

```
SLC_ULONG SLCAPI SlcTDesGenerateKey(
                    IN      const SLC_BYTE          * pbInitData,
                    IN      SLC_ULONG               ulKeyBitLen,
                    OUT     SLC_KEY                 * pSlcKey
                    );
```

参数说明：

pbInitData	以前的使用的无格式密钥。16 字节。可以为 NULL。 如果取值为 NULL，则此函数将生成随机数作为密钥。
ulKeyBitLen	密钥位数。可取值 112(SLC_TDES_KEY_BIT_LEN)。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE.
pSlcKey	传入一个 SLC_KEY 变量的地址。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.14 SlcTDesEnc

TDES 加密函数。使用 SLC_KEY 格式的 TDES 密钥。

```
SLC_ULONG SLCAPI SlcTDesEnc(
                    IN      SLC_BYTE            byMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB, SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
SlcKey	SLC_KEY 格式的 TDES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待加密的数据（明文）。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。

	出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.15 SlcTDesDec

TDES 解密函数。使用 SLC_KEY 格式的 TDES 密钥。

```
SLC_ULONG SLCAPI SlcTDesDec(
                    IN      SLC_BYTE            byMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbIv,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byMode	加密模式。 可取值：SLC_MODE_ECB，SLC_MODE_CBC. 出错返回值：SLC_ERROR_INVALID_MODE。
SlcKey	SLC_KEY 格式的 TDES 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbIv	初始化向量。 当 byMode 参数取值 SLC_MODE_ECB 时，此参数可为 NULL；如非 NULL 也

	不会被使用，也不报错。 当 byMode 参数取值 SLC_MODE_CBC 时，此参数应指定 8 字节的初始化向量缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。长度必须为 8 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	解密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.16 SlcSha1Init

用 SHA-1 算法计算数据的 HASH 值时，调用此函数对计算过程所用的 CONTEXT 进行初始化。

```
SLC_ULONG SLCAPI SlcSha1Init(
                        OUT     SLC_HASH_CTX            * pHashCtx
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。

返回值说明：
成功时返回 SLC_SUCCESS。

其它可能的返回值，请参阅“参数说明”部分。

4.17 SlcSha1Update

用 SHA-1 算法计算数据的 HASH 值时，调用此函数输入要处理的数据。
使用前，应调用 SlcSha1Init 函数初始化一个 SLC_HASH_CTX 变量。
如果数据较长，可将数据分块，每次调用此函数处理一个数据块。数据块的长度不限。

```
SLC_ULONG SLCAPI SlcSha1Update(
                        IN OUT  SLC_HASH_CTX            * pHashCtx,
                        IN      SLC_BYTE                * pbData,
                        IN      SLC_ULONG               ulDataLen
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。 使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0，但如果数据总长度也是 0，则输出结果不确定，但不报错。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.18 SlcSha1Final

用 SHA-1 算法计算数据的 HASH 值时，调用此函数结束计算过程，并返回数据的摘要。所得摘要长度为 20 字节。

```
SLC_ULONG SLCAPI SlcSha1Final(
                        IN OUT  SLC_HASH_CTX            * pHashCtx,
                        OUT     SLC_BYTE                * pbOutBuf
                        IN      SLC_ULONG               ulOutBufLen,
```

```
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。 使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 20（SLC_SHA1_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.19 SlcSha1

如果数据不长，可调用此函数一次性完成输入数据摘要计算。所得数据摘要的长度为 20 字节。

```
SLC_ULONG SLCAPI SlcSha1(
                    IN      SLC_BYTE            * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0。但如果数据长度是

	0，则输出结果不确定，不报错。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 20（SLC_SHA1_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.20 SlcSha256Init

用 SHA-256 算法计算数据的 HASH 值时，调用此函数对计算过程所用的 CONTEXT 进行初始化。

```
SLC_ULONG SLCAPI SlcSha256Init(
                        OUT     SLC_HASH_CTX            * pHashCtx
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.21 SlcSha256Update

用 SHA-256 算法计算数据的 HASH 值时，调用此函数输入要处理的数据。
使用前，应调用 SlcSha256Init 函数初始化一个 SLC_HASH_CTX 变量。
如果数据较长，可将数据分块，每次调用此函数处理一个数据块。数据块的长度不限。

```
SLC_ULONG SLCAPI SlcSha256Update(
                        IN OUT   SLC_HASH_CTX            * pHashCtx,
                        IN       SLC_BYTE                * pbData,
                        IN       SLC_ULONG               ulDataLen
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。 使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0，但如果数据总长度也是 0，则输出结果不确定，但不报错。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.22 SlcSha256Final

用 SHA-256 算法计算数据的 HASH 值时，调用此函数结束计算过程，并返回数据的摘要。所得摘要长度为 32 字节。

```
SLC_ULONG SLCAPI SlcSha256Final(
                        IN OUT   SLC_HASH_CTX            * pHashCtx,
                        OUT      SLC_BYTE                * pbOutBuf
                        IN       SLC_ULONG               ulOutBufLen,
                        OUT      SLC_ULONG               * pulOutDataLen
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。 使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。

	出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 32（SLC_SHA256_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.23 SlcSha256

如果数据不长，可调用此函数一次性完成输入数据摘要计算。所得数据摘要的长度为 32 字节。

```
SLC_ULONG SLCAPI SlcSha256(
                IN      SLC_BYTE            * pbData,
                IN      SLC_ULONG           ulDataLen,
                OUT     SLC_BYTE            * pbOutBuf
                IN      SLC_ULONG           ulOutBufLen,
                OUT     SLC_ULONG           * pulOutDataLen
                );
```

参数说明：

pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0。但如果数据长度是 0，则输出结果不确定，不报错。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 32（SLC_SHA256_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该

	变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.24 SlcMd5Init

用 MD5 算法计算数据的 HASH 值时，调用此函数对计算过程所用的 CONTEXT 进行初始化。

```
SLC_ULONG SLCAPI SlcMd5Init(
                        OUT     SLC_HASH_CTX            * pHashCtx
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.25 SlcMd5Update

用 MD5 算法计算数据的 HASH 值时，调用此函数输入要处理的数据。
使用前，应调用 SlcMd5Init 函数初始化一个 SLC_HASH_CTX 变量。

```
SLC_ULONG SLCAPI SlcMd5Update(
                        IN OUT  SLC_HASH_CTX            * pHashCtx,
                        IN      SLC_BYTE                * pbData,
                        IN      SLC_ULONG               ulDataLen
                        );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。

	使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0，但如果数据总长度也是 0，则输出结果不确定，但不报错。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.26 SlcMd5Final

用 MD5 算法计算数据的 HASH 值时，调用此函数结束计算过程，并返回数据的摘要。所得摘要长度为 16 字节。

```
SLC_ULONG SLCAPI SlcMd5Final(
                    IN OUT   SLC_HASH_CTX          * pHashCtx,
                    OUT      SLC_BYTE              * pbOutBuf,
                    IN       SLC_ULONG             ulOutBufLen,
                    OUT      SLC_ULONG            * pulOutDataLen
                    );
```

参数说明：

pHashCtx	SLC_HASH_CTX 型变量的地址。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER。 使用未初始化的 SLC_HASH_CTX 变量会导致内存访问错误。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 16（SLC_MD5_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：

成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.27 SlcMd5

如果数据不长，可调用此函数一次性完成输入数据摘要计算。所得数据摘要的长度为 16 字节。

```
SLC_ULONG SLCAPI SlcMd5(
                        IN      SLC_BYTE            * pbData,
                        IN      SLC_ULONG           ulDataLen,
                        OUT     SLC_BYTE            * pbOutBuf
                        IN      SLC_ULONG           ulOutBufLen,
                        OUT     SLC_ULONG           * pulOutDataLen
                        );
```

参数说明：

pbData	存放待处理数据的缓冲区。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulDataLen	待输出数据的字节数。数值不限。数据长度可为 0。但如果数据长度是 0，则输出结果不确定，不报错。
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能小于 16（SLC_MD5_DIGEST_LEN）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.28 SlcRsaGenerateKey

生成 SLC_KEY 格式的 RSA 公私钥对。

```
SLC_ULONG SLCAPI SlcRsaGenerateKey(
                        IN      SLC_ULONG               ulKeyBitLen,
                        OUT     SLC_KEY                 * pSlcPubKey,
                        OUT     SLC_KEY                 * pSlcPriKey
                        );
```

参数说明：

ulKeyBitLen	密钥位数。可取值 1024，2048，4096(SLC_RSA_KEY_BIT_1024，SLC_RSA_KEY_BIT_2048，SLC_RSA_KEY_BIT_4096)。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE.
pSlcPubKey	传入一个 SLC_KEY 变量的地址，用于存放公钥。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pSlcPriKey	传入一个 SLC_KEY 变量的地址，用于存放私钥。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.29 SlcRsaPubEnc

使用 SLC_KEY 格式的 RSA 公钥对数据进行加密。

```
SLC_ULONG SLCAPI SlcRsaPubEnc(
                        IN      SLC_BYTE                byPadMode,
                        IN      SLC_KEY                 SlcKey,
                        IN      const SLC_BYTE          * pbData,
                        IN      SLC_ULONG               ulDataLen,
                        OUT     SLC_BYTE                * pbOutBuf
                        IN      SLC_ULONG               ulOutBufLen,
```

```
    OUT     SLC_ULONG               * pulOutDataLen
    );
```

参数说明：

byPadMode	填充模式。 可取值：SLC_PAD_MODE_NONE, SLC_PAD_MODE_PKCS_1_V1_5.
SlcKey	SLC_KEY 格式的 RSA 公钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 公钥(ECC 私钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 公钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbData	待加密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。必须大于 0。 如果 byPadMode 取值 SLC_PAD_MODE_PKCS_1_V1_5,则字节数必须小于等于(密钥位数/8 - 11); 如果 byPadMode 取值 SLC_PAD_MODE_NONE,则字节数必须等于(密钥位数/8)，且第一个字节的最高位为 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH，SLC_ERROR_INVALID_INPUT_DATA.
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比(密钥位数/8)小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：

成功时返回 SLC_SUCCESS。

其它可能的返回值，请参阅“参数说明”部分。

4.30 SlcRsaPriDec

使用 SLC_KEY 格式的 RSA 私钥对数据密文进行解密。

```
SLC_ULONG SLCAPI SlcRsaPriDec(
                        IN      SLC_BYTE            byPadMode,
                        IN      SLC_KEY             SlcKey,
                        IN      const SLC_BYTE      * pbData,
                        IN      SLC_ULONG           ulDataLen,
                        OUT     SLC_BYTE            * pbOutBuf
                        IN      SLC_ULONG           ulOutBufLen,
                        OUT     SLC_ULONG           * pulOutDataLen
                        );
```

参数说明：

byPadMode	填充模式。 可取值：SLC_PAD_MODE_NONE, SLC_PAD_MODE_PKCS_1_V1_5.
SlcKey	SLC_KEY 格式的 RSA 公钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 私钥(ECC 公钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 私钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。必须等于（密钥位数/8）. 出错返回值：SLC_ERROR_INPUTDATA_LENGTH.
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。如果缓冲区长度不足，则会返回错误码。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.31 SlcRsaPriEnc

使用 SLC_KEY 格式的 RSA 私钥对数据进行加密。

```
SLC_ULONG SLCAPI SlcRsaPriEnc(
                        IN      SLC_BYTE            byPadMode,
                        IN      SLC_KEY             SlcKey,
                        IN      const SLC_BYTE      * pbData,
                        IN      SLC_ULONG           ulDataLen,
                        OUT     SLC_BYTE            * pbOutBuf
                        IN      SLC_ULONG           ulOutBufLen,
                        OUT     SLC_ULONG           * pulOutDataLen
                        );
```

参数说明：

byPadMode	填充模式。 可取值：SLC_PAD_MODE_NONE, SLC_PAD_MODE_PKCS_1_V1_5.
SlcKey	SLC_KEY 格式的 RSA 私钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 私钥(ECC 公钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 私钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbData	待加密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待加密的数据字节数。必须大于 0。 如果 byPadMode 取值 SLC_PAD_MODE_PKCS_1_V1_5,则字节数必须小于等于(密钥位数/8 - 11); 如果 byPadMode 取值 SLC_PAD_MODE_NONE,则字节数必须等于(密钥位数/8)，且第一个字节的最高位为 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH，SLC_ERROR_INVALID_INPUT_DATA.
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比(密钥位数/8)小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。

	可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.32 SlcRsaPubDec

使用 SLC_KEY 格式的 RSA 公钥对数据密文进行解密。

```
SLC_ULONG SLCAPI SlcRsaPubDec(
                    IN      SLC_BYTE            byPadMode,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbData,
                    IN      SLC_ULONG           ulDataLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulOutBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

byPadMode	填充模式。 可取值：SLC_PAD_MODE_NONE，SLC_PAD_MODE_PKCS_1_V1_5.
SlcKey	SLC_KEY 格式的 RSA 公钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 公钥(ECC 私钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 公钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbData	待解密的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待解密的数据字节数。必须等于（密钥位数/8）. 出错返回值：SLC_ERROR_INPUTDATA_LENGTH.
pbOutBuf	加密结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。如果缓冲区长度不足，则会返回错误码。

	出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.33 SlcRsaSign

使用 RSA 私钥对数据做数字签名。

```
SLC_ULONG SLCAPI SlcRsaSign(
                    IN      SLC_BYTE            byPadMode,
                    IN      SLC_ULONG           ulHashAlgo,
                    IN      SLC_KEY             SlcPriKey,
                    IN      const SLC_BYTE      * pbMessage,
                    IN      SLC_ULONG           ulMessageLen,
                    OUT     SLC_BYTE            * pbOutBuf
                    IN      SLC_ULONG           ulSignatureBufLen,
                    OUT     SLC_ULONG           * pulSignatureLen
                    );
```

参数说明：

byPadMode	填充模式。可取值： SLC_PAD_MODE_PKCS_1_V1_5. 出错返回值：SLC_ERROR_INVALID_MODE。
byHashAlgo	HASH 算法 ID. 可取值： SLC_HASH_ALGO_SHA1, SLC_HASH_ALGO_SHA256, SLC_HASH_ALGO_MD5。 出错返回值：SLC_ERROR_INVALID_HASH_ALGO。
SlcPriKey	SLC_KEY 格式的 RSA 私钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 私钥(ECC 公钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 私钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbMessage	待签名的数据。不可为 NULL。

	出错返回值：SLC_ERROR_INVALID_PARAMETER
ulMessageLen	待签名的数据字节数。不可为 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH.
pbSignatureBuf	签名结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulSignatureBufLen	输出缓冲区的字节数。长度不能比(密钥位数/8)小。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulSignatureLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.34 SlcRsaVerify

使用 RSA 公钥对数据签名做检验。

```
SLC_ULONG SLCAPI SlcRsaVerify(
                        IN      SLC_BYTE            byPadMode,
                        IN      SLC_ULONG           ulHashAlgo,
                        IN      SLC_KEY             SlcPubKey,
                        IN      const SLC_BYTE      * pbMessage,
                        IN      SLC_ULONG           ulMessageLen,
                        IN      const SLC_BYTE      * pbSignature,
                        IN      SLC_ULONG           ulSignatureLen
                        );
```

参数说明：

byPadMode	填充模式。可取值： SLC_PAD_MODE_PKCS_1_V1_5. 出错返回值：SLC_ERROR_INVALID_MODE。
byHashAlgo	HASH 算法 ID. 可取值：SLC_HASH_ALGO_SHA1, SLC_HASH_ALGO_SHA256, SLC_HASH_ALGO_MD5。 出错返回值：SLC_ERROR_INVALID_HASH_ALGO。

SlcPubKey	SLC_KEY 格式的 RSA 公钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 RSA 公钥(ECC 私钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 ECC 公钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbMessage	签名对应的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulMessageLen	签名对应的数据的字节数。
pbSignature	存放数字签名的缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulSignatureLen	数字签名的字节数。长度应等于（密钥位数/8）. 出错返回值：SLC_ERROR_INPUTDATA_LENGTH。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.35 SlcEccGenerateKey

生成 SLC_KEY 格式的 ECC 公私钥对。

```
SLC_ULONG SLCAPI SlcEccGenerateKey(
                    IN      SLC_ULONG           ulKeyBitLen,
                    OUT     SLC_KEY             * pSlcPubKey,
                    OUT     SLC_KEY             * pSlcPriKey
                    );
```

参数说明：

ulKeyBitLen	密钥位数。可取值 192(SLC_ECC_KEY_BIT_192)。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE.
pSlcPubKey	传入一个 SLC_KEY 变量的地址，用于存放公钥。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

pSlcPriKey	传入一个 SLC_KEY 变量的地址，用于存放私钥。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.36 SlcEccSign

使用 ECC 私钥对数据做数字签名。

```
SLC_ULONG SLCAPI SlcEccSign(
                    IN      SLC_ULONG           ulHashAlgo
                    IN      SLC_KEY             SlcPriKey,
                    IN      const SLC_BYTE      * pbMessage,
                    IN      SLC_ULONG           ulMessageLen,
                    OUT     SLC_BYTE            * pbSignatureBuf
                    IN      SLC_ULONG           ulSignatureBufLen,
                    OUT     SLC_ULONG           * pulSignatureLen
                    );
```

参数说明：

byHashAlgo	HASH 算法 ID. 可取值：SLC_HASH_ALGO_SHA1, SLC_HASH_ALGO_SHA256, SLC_HASH_ALGO_MD5。 出错返回值：SLC_ERROR_INVALID_HASH_ALGO。
SlcPriKey	SLC_KEY 格式的 ECC 私钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 ECC 私钥(RSA 公钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 RSA 私钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;
pbMessage	待签名的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulMessageLen	待签名的数据字节数。不可为 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH.

pbSignatureBuf	签名结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulSignatureBufLen	输出缓冲区的字节数。通常 ECC 签名结果在 56 字节左右，不会超过 128 字节。如果要一次性调用即获得签名结果，建议缓冲区长度不小于 128 字节。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulSignatureLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.37 SlcEccVerify

使用 ECC 公钥对数据签名做检验。

```
SLC_ULONG SLCAPI SlcEccVerify(
                    IN      SLC_ULONG           ulHashAlgo,
                    IN      SLC_KEY             SlcKey,
                    IN      const SLC_BYTE      * pbMessage,
                    IN      SLC_ULONG           ulMessageLen,
                    IN      const SLC_BYTE      * pbSig,
                    IN      SLC_ULONG           ulSigLen,
                    );
```

参数说明：

byHashAlgo	HASH 算法 ID. 可取值：SLC_HASH_ALGO_SHA1, SLC_HASH_ALGO_SHA256, SLC_HASH_ALGO_MD5。 出错返回值：SLC_ERROR_INVALID_HASH_ALGO。
SlcPubKey	SLC_KEY 格式的 ECC 公钥。不可为 NULL. 传入 NULL，则出错返回值：SLC_ERROR_INVALID_PARAMETER; 传入非 ECC 公钥(RSA 私钥、对称密钥)，则出错返回值：SLC_ERROR_BAD_KEY_TYPE; 传入 RSA 公钥，则出错返回值：SLC_ERROR_BAD_KEY_ALGORITHM;

pbMessage	签名对应的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulMessageLen	签名对应的数据的字节数。
pbSignature	存放签名结果的缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulSignatureLen	签名结果的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.38 SlcHmacGenerateKey

生成 SLC_KEY 格式的 HMAC 密钥。
如果有以前使用的无格式密钥，则可用以前的无格式密钥对所生成的 SLC_KEY 格式的密钥做初始化，使 SLC_KEY 密钥包含原来的无格式密钥。

```
SLC_ULONG SLCAPI SlcHmacGenerateKey(
                    IN      const SLC_BYTE          * pbInitData,
                    IN      SLC_ULONG               ulKeyBitLen,
                    IN      SLC_ULONG               ulAlgorithm,
                    OUT     SLC_KEY                 * pSlcKey
                    );
```

参数说明：

pbInitData	以前的使用的无格式密钥。可为 1~255 长度。可以为 NULL。 如果取值为 NULL，则此函数将生成随机数作为密钥。
ulKeyBitLen	密钥位数。为生成长度可以取（1~255）*8 位数.
ulAlgorithm	Hmac 密钥的类型，参考宏 Hmac 密钥类型定义.
pSlcKey	传入一个 SLC_KEY 变量的地址。不可为 NULL. 此函数负责分配密钥占用的缓冲区。使用之后，要调用 SlcFreeKey 函数释放此密钥。 出错返回值：SLC_ERROR_INVALID_PARAMETER.

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.39 SlcHmacRaw

Hmac 计算函数。使用 1~256 字节的无格式密钥。

```
SLC_ULONG SLCAPI SlcHmacRaw(
                        IN      SLC_BYTE            byAlgoHmac,
                        IN      const SLC_BYTE      * pbKey,
                        IN      SLC_ULONG           ulKeyLen,
                        IN      const SLC_BYTE      * pbData,
                        IN      SLC_ULONG           ulDataLen,
                        OUT     SLC_BYTE            * pbOutBuf
                        IN      SLC_ULONG           ulOutBufLen,
                        OUT     SLC_ULONG           * pulOutDataLen
                        );
```

参数说明：

bAlgoHmac	计算 HASH 算法。 可取值： SLC_CIPHER_ALGO_HMAC_MD5，SLC_CIPHER_ALGO_HMAC_SHA1，SLC_CIPHER_ALGO_HMAC_SHA256。 出错返回值：SLC_ERROR_INVALID_MODE。
pbKey	Hmac 密钥缓冲区。可为 1~256 字节。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
ulKeyLen	pbKey 密钥字节数。可取值 1~256 字节。 出错返回值：SLC_ERROR_INVALID_KEY_SIZE
pbData	待计算的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待计算的数据字节数。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。

ulOutBufLen	输出缓冲区的字节数。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.40 SlcHmac

Hmac 计算函数。使用 SLC_KEY 格式的 Hmac 密钥。

```
SLC_ULONG SLCAPI SlcHmac(IN      SLC_KEY              SlcKey,
                         IN      const SLC_BYTE       * pbData,
                         IN      SLC_ULONG            ulDataLen,
                         OUT     SLC_BYTE             * pbOutBuf
                         IN      SLC_ULONG            ulOutBufLen,
                         OUT     SLC_ULONG            * pulOutDataLen
                         );
```

参数说明：

SlcKey	SLC_KEY 格式的 HMAC 密钥。不可为 NULL. 取值为 NULL 时，出错返回值：SLC_ERROR_INVALID_PARAMETER. 密钥格式错误时，出错返回值： SLC_ERROR_BAD_KEY_VERSION ， SLC_ERROR_BAD_KEY_TYPE ， SLC_ERROR_BAD_KEY_ALGORITHM，SLC_ERROR_INVALID_KEY_SIZE.
pbData	待计算的数据。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER
ulDataLen	待计算的数据字节数。长度必须为 16 的倍数，且非 0。 出错返回值：SLC_ERROR_INPUTDATA_LENGTH
pbOutBuf	计算结果的输出缓冲区。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulOutBufLen	输出缓冲区的字节数。长度不能比 ulDataLen 小。

	出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulOutDataLen	变量地址。用于存放输出数据的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.41 SlcKeyToAesKey

将 SLC_KEY 格式的密钥转换为无格式的 AES 密钥。

```
SLC_ULONG SLCAPI SlcKeyToAesKey(
                    IN      SLC_KEY             SlcKey,
                    OUT     SLC_BYTE            * pbKeyBuf,
                    IN      SLC_ULONG           ulKeyBufLen,
                    OUT     SLC_ULONG           * pulKeyByteLen
                    );
```

参数说明：

SlcKey	SLC_KEY 格式的 AES 密钥。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER. 如果不是对称密钥，则出错返回：SLC_ERROR_BAD_KEY_TYPE; 如果是对称密钥，但不是 AES 的密钥，则出错返回：SLC_ERROR_BAD_KEY_ALGORITHM。
pbKeyBuf	输出缓冲区。用于存放转换后所得的无格式密钥。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulKeyBufLen	输出缓冲区的字节数。可取值 16，24，32（分别对应 128，192，256 位的密钥）。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulKeyByteLen	变量地址。用于存放所得无格式密钥的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.42 SlcKeyToDesKey

将 SLC_KEY 格式的密钥转换为无格式的 DES 密钥。

```
SLC_ULONG SLCAPI SlcKeyToDesKey(
                    IN      SLC_KEY             SlcKey,
                    OUT     SLC_BYTE            * pbKeyBuf,
                    IN      SLC_ULONG           ulKeyBufLen,
                    OUT     SLC_ULONG           * pulOutDataLen
                    );
```

参数说明：

SlcKey	SLC_KEY 格式的 DES 密钥。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER. 如果不是对称密钥，则出错返回：SLC_ERROR_BAD_KEY_TYPE; 如果是对称密钥，但不是 DES 的密钥，则出错返回：SLC_ERROR_BAD_KEY_ALGORITHM。
pbKeyBuf	输出缓冲区。用于存放转换后所得的无格式密钥。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulKeyBufLen	输出缓冲区的字节数。不应小于 8。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulKeyByteLen	变量地址。用于存放所得无格式密钥的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.43 SlcKeyToTDesKey

将 SLC_KEY 格式的密钥转换为无格式的 TDES 密钥。

```
SLC_ULONG SLCAPI SlcKeyToTDesKey(
                        IN      SLC_KEY             SlcKey,
                        OUT     SLC_BYTE            * pbKeyBuf,
                        IN      SLC_ULONG           ulKeyBufLen,
                        OUT     SLC_ULONG           * pulOutDataLen
                        );
```

参数说明：

SlcKey	SLC_KEY 格式的 TDES 密钥。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER. 如果不是对称密钥，则出错返回：SLC_ERROR_BAD_KEY_TYPE; 如果是对称密钥，但不是 TDES 的密钥，则出错返回：SLC_ERROR_BAD_KEY_ALGORITHM。
pbKeyBuf	输出缓冲区。用于存放转换后所得的无格式密钥。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulKeyBufLen	输出缓冲区的字节数。不应小于 16 字节。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulKeyByteLen	变量地址。用于存放所得无格式密钥的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.44 SlcKeyToHmacKey

将 SLC_KEY 格式的密钥转换为无格式的 Hmac 密钥。

```
SLC_ULONG SLCAPI SlcKeyToHmacKey(
                        IN      SLC_KEY             SlcKey,
                        OUT     SLC_BYTE            * pbKeyBuf,
                        IN      SLC_ULONG           ulKeyBufLen,
```

```
                    OUT     SLC_ULONG           * pulOutDataLen,
                    OUT     SLC_BYTE            * sbAlgorithm
                    );
```

参数说明：

SlcKey	SLC_KEY 格式的 Hmac 密钥。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER. 如果不是对称密钥，则出错返回：SLC_ERROR_BAD_KEY_TYPE; 如果是对称密钥，但不是 Hmac 的密钥，则出错返回：SLC_ERROR_BAD_KEY_ALGORITHM。
pbKeyBuf	输出缓冲区。用于存放转换后所得的无格式密钥。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulKeyBufLen	输出缓冲区的字节数。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulKeyByteLen	变量地址。用于存放所得无格式密钥的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。
sbAlgorithm	该密钥使用的 HASH 类型。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.45 SlcCheckKeyType

检查 SLC_KEY 格式的密钥的类型和算法与指定类型 ID，算法 ID 是否一致。如果一致，则返回 SLC_SUCCESS。
用于密钥的导入，以判断所导入的密钥与随后的用途是否一致。工具程序用。

```
SLC_ULONG SLCAPI SlcCheckKeyType (
                    IN      SLC_KEY             SlcKey,
                    IN      SLC_BYTE            byKeyType,
                    IN      SLC_BYTE            byAlgorithm
                    );
```

参数说明：

SlcKey	SLC_KEY 格式的密钥。不可为 NULL.

	出错返回值：SLC_ERROR_INVALID_PARAMETER.
byKeyType	密钥类型 ID。可取值：SLC_KEY_SYMMETRIC（对称密钥），SLC_KEY_PUBLIC（公钥），SLC_KEY_PRIVATE（私钥）。 如传入其它数值，不视为错误。
byAlgorithm	密钥算法 ID。 可取值： SLC_CIPHER_ALGO_AES, SLC_CIPHER_ALGO_DES, SLC_CIPHER_ALGO_TDES, SLC_CIPHER_ALGO_RSA, SLC_CIPHER_ALGO_ECC. 如传入其它数值，不视为错误。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.46 SlcGetKeySize

获取 SLC_KEY 格式的密钥的字节数。用于密钥的导出。工具程序用。

```
SLC_ULONG SLCAPI SlcGetKeySize(
                        IN      SLC_KEY         SlcKey,
                        );
```

参数说明：

SlcKey	SLC_KEY 格式的密钥。不可为 NULL. 出错返回值：0.

返回值说明：
成功时返回一个非零的数值。如果返回 0，则表示传入的密钥有误。
注意：此函数返回 0 表示出错。（SLC_SUCCESS 的值也是 0，不要混淆。）

4.47 SlcGetKeyBitLength

获取 SLC_KEY 格式的密钥的密钥位数。工具程序用。

```
SLC_ULONG SLCAPI SlcGetKeyBitLength(
                        IN      SLC_KEY                 SlcKey
                        );
```

参数说明：

SlcKey	SLC_KEY 格式的密钥。不可为 NULL. 出错返回值：0.

返回值说明：
成功时返回一个非零的数值。如果返回 0，则表示传入的密钥有误。
注意：此函数返回 0 表示出错。（SLC_SUCCESS 的值也是 0，不要混淆。）

4.48 SlcExportKey

将 SLC_KEY 格式的密钥转存到缓冲区中。用于密钥的导出。
工具程序用。

```
SLC_ULONG SLCAPI SlcExportKey(
                        IN      SLC_KEY                 SlcKey,
                        OUT     SLC_BYTE                * pbOutBuf
                        IN      SLC_ULONG               ulOutBufLen,
                        OUT     SLC_ULONG               * pulOutDataLen
                        );
```

参数说明：

SlcKey	SLC_KEY 格式的密钥。不可为 NULL. 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbKeyBuf	输出缓冲区。用于存放 SLC_KEY 格式的密钥。不可为 NULL。 出错返回值：SLC_ERROR_INVALID_PARAMETER。
ulKeyBufLen	输出缓冲区的字节数。所需缓冲区长度可事先用 SlcGetKeySize 函数获取。 出错返回值：SLC_ERROR_INSUFFICIENT_BUFFER。
pulKeyByteLen	变量地址。用于存放所输出的 SLC_KEY 格式密钥的字节数。当输出缓冲区长度不足时，该变量可返回所需缓冲区的字节数。 可以传入 NULL，这时表示不需要返回输出数据的字节数。

返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分。

4.49 SlcImportKey

将缓冲区中的密钥转存到 SLC_KEY 格式的密钥指针中，此函数负责分配密钥占用的内存。导入的密钥使用后要释放。
用于密钥的导入。工具程序用。

```
SLC_ULONG SLCAPI SlcImportKey(
                        OUT     SLC_KEY                 * pSlcKey,
                        IN      const SLC_BYTE          * pbInputBuf,
                        IN      SLC_ULONG               ulInputDataLen
                        );
```

参数说明：

pSlcKey	SLC_KEY 型变量的地址。不可为 NULL. 此函数负责为密钥分配存储空间。导入的密钥用后要调用 SlcFreeKey 函数释放。 出错返回值：SLC_ERROR_INVALID_PARAMETER.
pbInputBuf	存放密钥内容的缓冲区。不可为 NULL。
ulInputDataLen	存放密钥的缓冲区中，有效数据的字节数。

说明：
返回值说明：
成功时返回 SLC_SUCCESS。
其它可能的返回值，请参阅“参数说明”部分即下面的附加说明。

此函数会检查数据的长度和格式。可能返回下述返回值：
SLC_ERROR_INPUTDATA_LENGTH,（数据长度错误）
SLC_ERROR_BAD_KEY_VERSION,（密钥版本信息错误）
SLC_ERROR_BAD_KEY_TYPE,（密钥类型错 ID 错误）
SLC_ERROR_BAD_KEY_FORMAT,（密钥内部的各字段内容不匹配，如：密钥类型 ID 字段与密钥长度字段不匹配。）
SLC_ERROR_BAD_KEY_ALGORITHM,（密钥的算法 ID 错误）

4.50 SlcFreeKey

释放 SLC_KEY 格式的密钥所占所有的存储空间。
时所用 SlcXXXGenerateKey 系列函数生成的密钥，使用 SlcImportKey 函数导入的密钥在使用后都应用此函数释放。

```
SLC_ULONG SLCAPI SlcFreeKey(
                        IN OUT  SLC_KEY                 * pSlcKey
                        );
```

参数说明：

pSlcKey	SLC_KEY 型变量的地址。可为 NULL，并执行成功。

返回值说明：
此函数只会返回 SLC_SUCCESS。
如果传入的变量地址非 NULL，并且该变量的原始值是不是 NULL，则该变量在函数返回后会被设置为 NULL.
如果传入的变量地址非 NULL，并且该变量的原始值是 NULL，则函数返回 SLC_SUCCESS，且该变量的值仍是 NULL。