

# CV183x/CV182x/CV181x/CV180x CIPHER API 参考

Version: 1.2.0

Release date: 2022-10-19

© 2022 北京晶视智能科技有限公司

本文件所含信息归北京晶视智能科技有限公司所有。

未经授权,严禁全部或部分复制或披露该等信息。

confidential

深圳艇十



### 法律声明

本数据手册包含北京晶视智能科技有限公司(下称"晶视智能")的保密信息。未经授权,禁止使用或披露本数据手册中包含的信息。如您未经授权披露全部或部分保密信息,导致晶视智能遭受任何损失或损害,您应对因之产生的损失/损害承担责任。

本文件内信息如有更改, 恕不另行通知。晶视智能不对使用或依赖本文件所含信息承担任何责任。

本数据手册和本文件所含的所有信息均按"原样"提供,无任何明示、暗示、法定或其他形式的保证。晶视智能特别声明未做任何适销性、非侵权性和特定用途适用性的默示保证,亦对本数据手册所使用、包含或提供的任何第三方的软件不提供任何保证;用户同意仅向该第三方寻求与此相关的任何保证索赔。此外,晶视智能亦不对任何其根据用户规格或符合特定标准或公开讨论而制作的可交付成果承担责任。

Confidential for With Mark



### 修订记录

Revision	Date	Author	Description	+10
1.2.0	2022-10-19	767	Initial	6//
1.2.1	2022-11-14	徐龙	review	
		Co		

深圳種

Confidential for Athlet



## 目录

2)	13.8	187	_	121
法律	声明			yen1
修订	记录	36 <sub>7</sub>		2
目录				3
1	概述			4
	1.1. 概述			4
	1.2. 使用流程			5
	1.2.1. 单包数据点	µ解密		5
	1.2.2. 多包数据点	µ解密		5
	1.2.3. HASH 计算	拿		6
	1.2.5. 产生随机数	汝		7
		· ·	W)	
	1.2.7. RSA 签名。	及验签操作步骤	<i>K</i> <sup>n</sup>	8
2	○′ API 参考			9
2.	数据类型	$\sim g_{\rm e} v_{\rm tr}$		<u>,</u> 25
3.	错误码	$p_{T_{T_1}}$	$Cou_{ET}$	26

for 淡湖柳



#### 1 概述

### 1.1. 概述

Confidential CIPHER 是晶视智能数字媒体处理平台提供的安全算法模块,提供对称式加解密 算法包括 AES/DES/SM4, 不对称加解密算法 RSA (Note SW), 随机数生成, 以 及摘要算法包插 HASH, HMAC, 主要用于对音视频码流进行加解密保护, 认证用 户合法性等场景, 各功能划分如下:

#### 对称加密算法

• AES: 支持 ECB/CBC/CTR/ CCM/GCM (Note SW)等工作模式。其中 CCM/GCM

模式下,加解密结束后需获取一次 TAG 值。

- DES: 支持 ECB/CBC/CTR/ CFB/OFB (Note SW)等工作模式, 其中 CFB 和 OFB 模式支持的位宽可为 1/8/64
  - SM4:支持 ECB/CBC/CTR 等工作模式

以上算法除了 CTR/ CCM/GCM, 其它算法、模式的数据长度必须按块大小对 齐, CCM/GCM 的 N、A 需要靠软件按标准把各个字段封装成块大小对齐的数 据块;

#### 不对称加解密算法

RSA (Note SW): 支持密钥位宽 1024/2048/3072/4096

RSA 密钥位宽 1024 及以下算法为业界已知不安全算法, 应禁止使用。

#### 随机数生成

• RNG: 高速率获取随机数

#### 摘要算法

- HASH: 支持 SHA1/SHA2/ SHA512/SM3 (Note SW);
- for 深圳種一 HMAC: 支 HMAC1/HMAC224/HMAC256/HMAC384/HMAC512 (Note SW);

SHA1 算法安全性较低,不能应用在参与生成"数字签名"的场景,推荐使用 Confident SHA2 (256 位及以上) 算法。

Confidential for ixillife



1.2.1. 单包数据加解密 场景说明 当物理内存中有一段码流数据需要进行加/解密时、获取 其物理地址后,在用户层调用 CIPHER 模块实现单包数据加/解密。

#### 工作流程

对数据进行对称的 AES/DES/SM4 加解密的过程如下:

步骤 1: CIPHER 设备初始化。调用接口 CVI\_UNF\_CIPHER\_Init 完成。

步骤 2: 获取 CIPHER 句柄。调用接口 CVI UNF CIPHER CreateHandle 完成。

步骤 3: 配置 CIPHER 控制信息. Confidential for TRHIMET 包含密钥、初始向量、加密算法、工作模式等信息。 调用接口 CVI UNF CIPHER ConfigHandle 或 CVI UNF CIPHER ConfigHandleEx 完成。

步骤 4:对数据进行加/解密。调用以下任一接口进行加解密。

- 单包加密, CVI\_UNF\_CIPHER\_Encrypt
- 单包解密, CVI\_UNF\_CIPHER\_Decrypt

步骤 5: 若使用 CCM、GCM (Note SW)模式, 调用接口 CVI UNF CIPHER GetTag 获取 TAG 值。

步骤 6: 销毁 CIPHER 句柄。调用接口 CVI UNF CIPHER DestroyHandle 完成。

步骤 7: 关闭 CIPHER 设备。调用接口 CVI UNF CIPHER Deinit 完成。

#### 注意事项

#### 1.2.2. 多包数据加解密

#### 场景说明

Confidential

. // 全內仔中有多段码流数据需要进行加/解密时,获取 其物理地址后, 在用户层调用 CIPHER 模块实现多包数据加/解密。 :**流程** 工作流程

对数据进行对称的 AES/DES/SM4 加解密的过程如下:

步骤 1: CIPHER 设备初始化。调用接口 CVI UNF CIPHER Init 完成。

for 深圳艇士 步骤 2: 获取 CIPHER 句柄。调用接口 CVI UNF CIPHER CreateHandle 完成。

步骤 3: 配置 CIPHER 控制信息.

包含密钥、初始向量、加密算法、工作模式等信息。 调用接口 CVI UNF CIPHER ConfigHandle 或 CVI\_UNF\_CIPHER\_ConfigHandleEx 完成。

步骤 4: 对数据进行加/解密。调用以下任一接口进行加解密。

- 多包加密, CVI\_UNF\_CIPHER\_EncryptMulti
- 多包解密, CVI\_UNF\_CIPHER\_DecryptMulti

步骤 5: 销毁 CIPHER 句柄。调用接口 CVI UNF CIPHER DestroyHandle 完成。

Confidential for This will be the confidential for 步骤 6:关闭 CIPHER 设备。调用接口 CVI\_UNF\_CIPHER\_Deinit 完成。 Confidential for Fride 注意事项

1.2.3. HASH 计算

### 场景说明

计算数据的 HASH 值, 可选择 SHA1/SHA2/ SHA512/SM3 (Note SW) 工作流程

步骤 1: CIPHER 设备初始化。调用接口 CVI\_UNF\_CIPHER\_Init 完成。

步骤 2: 获取 HASH 句柄, 选择 HASH 算法。 调用接口 CVI\_UNF\_CIPHER\_HashInit 完成。

步骤 3: 输入数据, 逐个数据块依次计算 HASH 值。 调用接口 CVI\_UNF\_CIPHER\_HashUpdate 完成。

步骤 4: 如果摘要未计算完成,再次执行步骤 3。

步骤 5:完成摘要计算、结束输入、获取计算结果。 调用接口 CVI UNF CIPHER HashFinal 完成

confidential for TRIMET 步骤 6:关闭 CIPHER 设备。调用接口 CVI\_UNF\_CIPHER\_Deinit 完成。

# 注意事项



#### 1.2.4. HMAC 计算 (NOTE SW)

#### 场景说明

基于 HASH 算法, 计算数据的 HMAC 值

#### 工作流程

Jonfidential for TRHIME 步骤 1: CIPHER 设备初始化。调用接口 CVI UNF CIPHER Init 完成。

步骤 2: 获取 HASH 句柄, 选择 HASH 算法并配置 HMAC 计算的密钥, 调用接口 CVI\_UNF\_CIPHER\_HashInit 完成。

步骤 3: 输入数据, 逐个数据块依次计算 HMAC 值。 调用接口 CVI UNF CIPHER HashUpdate 完成。

步骤 4: 如果摘要未计算完成。再次执行步骤 3。

步骤 5:完成摘要计算, 结束输入, 获取 HMAC 计算结果。 调用接口 CVI UNF CIPHER HashFinal 完成

Confidential for Frille 步骤 6:关闭 CIPHER 设备。调用接口 CVI\_UNF\_CIPHER\_Deinit 完成。 Confidential for TRHIME

#### 注意事项

#### 1.2.5. 产生随机数

#### 场景说明

获取硬件产生的真随机数.

#### 工作流程

步骤 1: CIPHER 设备初始化。调用接口 CVI\_UNF\_CIPHER\_Init 完成。

步骤 2: 获取 256bits 随机数,

调用接口 CVI\_UNF\_CIPHER\_GetRandomNumber 完成。

步骤 3:关闭 CIPHER 设备。调用接口 CVI UNF CIPHER Deinit 完成。

#### 注意事项

## 1.2.6. RSA 加解密操作步骤 (NOTE SW)

#### 场景说明

对数据进行 RSA 不对称算法加解密。使用公钥加密的数据,必须使用私钥进行 解密。反之,使用私钥加密的数据,必须使用公钥解密。

for深圳種十



#### 工作流程

步骤 1: CIPHER 设备初始化。调用接口 CVI\_UNF\_CIPHER\_Init 完成。

步骤 2:对数据进行加解密或签名验证。

根据使用的密钥不同, 调用以下任一接口进行加解密、签名验证、生 成密钥对等。

- 公钥加密: CVI\_UNF\_CIPHER\_RsaPublicEncrypt
- 私钥解密:CVI\_UNF\_CIPHER\_RsaPrivateDec
- 私钥加密:CVI\_UNF\_CIPHER\_RsaPrivateEnc
- 公钥解密: CVI UNF CIPHER RsaPublicDec
- 私钥签名:CVI\_UNF\_CIPHER\_RsaSign
- 公钥验证: CVI UNF CIPHER RsaVerify

步骤 3:关闭 CIPHER 设备。调用接口 CVI UNF CIPHER Deinit 完成。

#### 注意事项

#### 1.2.7. RSA 签名及验签操作步骤

#### 场景说明

itial for ixillifet 对数据进行 RSA 签名及验签时,使用私钥进行数据签名,使用进行数据验签。

#### 工作流程

步骤 1: CIPHER 设备初始化。调用接口 CVI UNF CIPHER Init 完成。

步骤 2: 对数据进行签名验证。

- 私钥签名:CVI\_UNF\_CIPHER\_RsaSign
- 公钥验证: CVI UNF CIPHER RsaVerify

步骤 3:关闭 CIPHER 设备。调用接口 CVI\_UNF\_CIPHER\_Deinit 完成。

# 注意事项 confidential for TRIMET

Confidential

for 淡湖随



#### 2 API 参考

#### CIPHER 提供以下 API:

- CVI\_UNF\_CIPHER\_Init: 初始化 CIPHER 模块。
- CVI UNF CIPHER\_Deinit: 去初始化 CIPHER 模块。
- CVI\_UNF\_CIPHER\_Open: 打开 CIPHER 模块。
- CVI\_UNF\_CIPHER\_Close: 关闭 CIPHER 模块。
- CVI UNF CIPHER CreateHandle: 创建 Cipher 句柄。
- CVI\_UNF\_CIPHER\_DestroyHandle: 销毁已存在的 CIPHER 句柄。
- CVI\_UNF\_CIPHER\_ConfigHandle: 配置 CIPHER 控制信息。

fidentia

- CVI UNF CIPHER ConfigHandleEx: 配置 CIPHER 控制信息(扩展)。
- CVI UNF CIPHER GetHandleConfig: 获取 CIPHER 配置信息。 Confidential for This was confidential
- CVI\_UNF\_CIPHER\_Encrypt: 单包数据加密功能。
- CVI\_UNF\_CIPHER\_Decrypt: 单包数据解密功能。
- CVI\_UNF\_CIPHER\_EncryptVir: 对数据进行加密。
- CVI\_UNF\_CIPHER\_DecryptVir: 对数据进行解密。
- CVI\_UNF\_CIPHER\_EncryptMulti: 多包数据加密功能。
- CVI UNF CIPHER DecryptMulti: 多包数据解密功能。
- CVI UNF CIPHER HashInit: HASH、HMAC 计算初始化功能。
- CVI UNF CIPHER HashUpdate: HASH、HMAC 计算数据输入功能。
- CVI UNF CIPHER HashFinal: HASH、HMAC 计算最终结果输出功能。
- CVI\_UNF\_CIPHER\_GetRandomNumber: 获取随机数功能。
- CVI\_UNF\_CIPHER\_GetTag: 获取 TAG 值。
- CVI\_UNF\_CIPHER\_RsaPublicEncrypt: 使用公钥对明文进行加密。
- CVI\_UNF\_CIPHER\_RsaPrivateDecrypt: 使用私钥对密文进行解密。
- CVI\_UNF\_CIPHER\_RsaPrivateEncrypt: 使用私钥对明文进行加密。
- CVI\_UNF\_CIPHER\_RsaPublicDecrypt: 使用公钥对密文进行解密。
- CVI\_UNF\_CIPHER\_RsaSign: 使用私钥对用户数据进行签名。
- gor 深圳腫土 confidentie. CVI\_UNF\_CIPHER\_RsaVerify: 使用公钥对用户数据进行合法性及完整性验证。
  - CVI\_UNF\_CIPHER\_KladEncryptKey: 使用 KLAD 对透明密钥进行加密。

confidential for ist illimet



## CVI\_UNF\_CIPHER\_Init Confidentia

【描述】

初始化 CIPHER 模块。

【语法】

CVI S32 CVI UNF CIPHER Init(void);

【参数】

无。

【返回值】

返回值	描述	
0	成功	
非 0	参考错误码	

#### CVI\_UNF\_CIPHER\_Deinit

【描述】

去初始化 CIPHER 模块。

【语法】

for深圳種子 CVI\_S32 CVI\_UNF\_CIPHER\_DeInit(void);

【参数】

无。

【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_Open

【描述】

打开 CIPHER 模块。

【语法】

【参数】

无。

#define CVI_UNF_CIPHE	R_Open(CVI_VOID)
CVI_UNF_CIPHER_Init(CV	/I_VOID);
【参数】	
无。	
【返回值】	Yeur,
返回值	描述

#### Specifications are subject to change without notice

0 35 11/1/19	成功				
(非 O	参考错误码				
CVI_UNF_CIPHER_Close					
【描述】					
关闭 CIPHER 模块。					

# 关闭 CIPHER 模块。 【语法】

#define CVI\_UNF\_CIPHER\_Close(CVI\_VOID)

CVI\_UNF\_CIPHER\_DeInit(CVI\_VOID);

【参数】

无。

【返回值】

返回值	描述			
0	成功			
非 0	参考错误码			
_UNF_CIPHER_CreateHandle 【描述】				
创建一路的 Cipher 句柄。 【语法】	dential			

#### CVI\_UNF\_CIPHER\_CreateHandle

fidential for Athlet CVI\_S32 CVI\_UNF\_CIPHER\_CreateHandle(CVI\_HANDLE\* phCipher, const CVI\_UNF\_CIPHER\_ATTS\_S \*pstCipherAttr);

#### 【参数】

参数名称	描述	输入/输出
phCipher	CIPHER 句柄指针	输出
pstCipherAtt	CIPHER 属性指针	输入

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码
_UNF_CIPHER_DestroyH 【描述】 销毁一路 CIPHER。	landle for thinker

## CVI UNF CIPHER DestroyHandle Confidential



#### 【语法】

#### 【参数】

u	itions are subject	to change without hotice		
	【语法】		证别便	爱圳随
		NF_CIPHER_DestroyH	landle(CVI_HANDLE hCipher);	
	【参数】	: 2)	: 2	
	参数名称	描述	输入/输出	
	hCipher	CIPHER 句相	两 输入 CONT	

#### 【返回值】

返回值	描述	
0	成功	
非 0	参考错误码	

#### CVI\_UNF\_CIPHER\_ConfigHandle

【描述】

配置 CIPHER 控制信息。详细配置请参见结构体 CVI\_UNF\_CIPHER\_CTRL\_S。 otial for \*\*\* #### 【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_ConfigHandle(CVI\_HANDLE hCipher,

CVI UNF CIPHER CTRL S\* pstCtrl);

#### 【参数】

12 201	1011	1011
参数名称	描述	输入/输出
hCipher	CIPHER 句柄。	输入
pstCtrl	控制信息指针	输入

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

### CVI\_UNF\_CIPHER\_ ConfigHandleEx

【描述】

配置 CIPHER 控制信息。详细配置请参见结构体

CVI UNF CIPHER CTRL EX S.

【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_ConfigHandleEx(CVI\_HANDLE hCipher,



#### CVI\_UNF\_CIPHER\_CTRL\_EX\_S\* pstExCtrl);

### 【参数】

ations are subjec	t to change	Without house			
	HER_CTRL	_EX_S* pstExCtrl);	随		深圳随土
《参数》		802			for v
参数名称		描述	输入/输出	1 12	)
hCipher	- S	CIPHER 句柄。	输入	fident	
pstExCtrl	$Co_{II}$	控制扩展信息指针。	输入 🗘		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_GetHandleConfig

【描述】

获取 CIPHER 信道对应的配置信息。

【语法】

#### 【参数】

	【语法】			
C	VI_S32 CVI_UNF_CIPH	ER_GetHandleConfig(C	VI_HANDLE hCipher,	
C	VI_UNF_CIPHER_CTRL	_S* pstCtrl);		
80	【参数】	· 1 for	1	Eor
,	参数名称	描述	输入/输出	
	hCipher conf	CIPHER 句柄。	输入 ( )	
	pstCtrl	CIPHER 信道的配置	输出	
		信息		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_Encrypt

for 深圳随土 CVI\_S32 CVI\_UNF\_CIPHER\_Encrypt(CVI\_HANDLE hCipher, CVI\_U32 u32SrcPhyAddr, Confident



#### CVI\_U32 u32DestPhyAddr, CVI\_U32 u32ByteLength);

Speeme	ations are subject to change CVI_U32 u32DestPhyAc		ngth);	10000000000000000000000000000000000000
	【参数】	描述。	输入/输出	
	hCipher	CIPHER 句柄。	输入	
	u32SrcPhyAddr	源数据(待加密的数 据)的物理地址	输入 〇	
	u32DestPhyAddr	存放加密结果的物理 地址	输入	
	u32ByteLength	数据的长度(单位: 字节)。	输入	

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_Decrypt

【描述】

对数据进行解密。

【语法】

tial for \*\*\* thinket CVI\_S32 CVI\_UNF\_CIPHER\_Decrypt(CVI\_HANDLE hCipher, CVI\_U32 u32SrcPhyAddr,

CVI\_U32 u32DestPhyAddr, CVI\_U32 u32ByteLength);

#### 【参数】

参数名称	描述	输入/输出	
hCipher	CIPHER 句柄。	输入	
u32SrcPhyAddr	源数据(待解密的数 据)的物理地址	输入	
u32DestPhyAddr	存放解密结果的物理 地址。	输入	
u32ByteLength	数据的长度(单位:	输入	
	字节)。	X	一通人
【返回值】			
返回值	描述		
0	成功	+121	
非0	参考错误码	Confidential	
	14		

#### 【返回值】

返回值		描述
0		成功。
非 0	61	参考错误码
	Com	
		14



## CVI\_UNF\_CIPHER\_EncryptVir Confidentia

【描述】

对数据进行加密。

【语法】

Confidential for ikillimet fidential for 深圳随 CVI\_S32 CVI\_UNF\_CIPHER\_EncryptVir(CVI\_HANDLE hCipher, const CVI\_U8 \*pu8SrcData, CVI\_U8 \*pu8DestData, CVI\_U32 u32ByteLength);

#### 【参数】

参数名称	描述	输入/输出	
hCipher	CIPHER 句柄。	输入	
*pu8SrcData	源数据(待加密的数 据)的虚拟地址。	输入	
*pu8DestData	存放加密结果的虚拟 地址	输出	
u32ByteLength	数据的长度(单位: 字节)。	输入 Confidential	一通小
【返回值】	采为		深圳
返回值	描述		
0	成功	ntial	
非0	参考错误码	confider.	
00,		0,	

#### 【返回值】

【返回值】	· · · · · · · · · · · · · · · · · · ·
返回值	描述
0	成功
非0	参考错误码

#### CVI\_UNF\_CIPHER\_DecryptVir

【描述】

对数据进行解密。

【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_DecryptVir(CVI\_HANDLE hCipher, const CVI\_U8 \*pu8SrcData, CVI\_U8 \*pu8DestData, CVI\_U32 u32ByteLength);

#### 【参数】

参数名称	描述	输入/输出	
hCipher	CIPHER 句柄。	输入	云州相
*pu8SrcData	源数据(待解密的数 据)的虚拟地址。	输入	EOI IK.
*pu8DestData	存放解密结果的虚拟 地址。。	输出	
Corr	15	Cor	•

ations are subject to change	without notice	
A.X	A.Y	
u32ByteLength	数据的长度(单位: 输 字节)。	7人 深圳/
  【返回值】	+ 1010 COL	Fox
返回值	描述	intial
0 005	成功	confider
非 0	参考错误码	001

#### 【返回值】

返回值	描述
0 confi	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_EncryptMulti

【描述】

进行多个包数据的加密。

【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_EncryptMulti(CVI\_HANDLE hCipher,

CVI\_UNF\_CIPHER\_DATA\_S

\*pstDataPkg, CVI\_U32 u32DataPkgNum);

#### 【参数】

【参数】 / /			
参数名称	描述	输入/输出	"运制模"
hCipher	CIPHER 句柄。	输入	602 1X
*pstDataPkg	待加密的数据包	输入	
u32DataPkgNum	待加密的数据包个 数。	输入 Confident	
	参数名称 hCipher *pstDataPkg	参数名称描述hCipherCIPHER 句柄。*pstDataPkg待加密的数据包u32DataPkgNum待加密的数据包个	参数名称描述输入/输出hCipherCIPHER 句柄。输入*pstDataPkg待加密的数据包输入u32DataPkgNum待加密的数据包个输入

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_DecryptMulti

【描述】

进行多个包数据的解密。

【语法】

Confidential for This was confidential CVI\_S32 CVI\_UNF\_CIPHER\_DecryptMulti(CVI\_HANDLE hCipher,

CVI\_UNF\_CIPHER\_DATA\_S

\*pstDataPkg, CVI\_U32 u32DataPkgNum);

#### 【参数】

ations are subject to change	without house		
【参数】	THI THE	+	云圳横十
参数名称	描述	输入/输出	8 O.Z.
hCipher	CIPHER 句柄。	输入	> -
*pstDataPkg	待解密的数据包。	输入	
u32DataPkgNum	待解密的数据包个 数。。	输入 (0)	

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_HashInit

【描述】初始化 HASH 模块。

#### 【语法】

I for \*\*\* Thinke t CVI\_S32 CVI\_UNF\_CIPHER\_HashInit(CVI\_UNF\_CIPHER\_HASH\_ATTS\_S \*pstHashAttr,

CVI\_HANDLE \*pHashHandle);

#### 【参数】

参数名称	描述	输入/输出
pstHashAttr	用于计算 hash 的结 构体参数	输入
pHashHandle	输出的 hash 句柄。	输出

#### 【返回值】

返回值	描述
0 ******	成功
<b>菲 0</b>	参考错误码

### Confidential CVI\_UNF\_CIPHER\_HashUpdate



#### 【描述】

计算 hash 值。

#### 【语法】

idential for ikillifet idential for Frimmer CVI\_S32 CVI\_UNF\_CIPHER\_HashUpdate(CVI\_HANDLE hHashHandle, CVI\_U8 \*pu8InputData, CVI\_U32 u32InputDataLen);

#### 【参数】

参数名称	描述	输入/输出	
hHashHandl	Hash 句柄	输入	
pu8InputData	输入数据缓冲。	输入	
u32InputDataLen	输入数据的长度,单	输入	
·	位: byte。		
【返回值】 <b>返回值</b>	描述	Confidential	
0	成功		
非 0	参考错误码	. dentiar	

#### 【返回值】

【返回值】	
返回值	描述
90	成功
anfidential 集0	参考错误码
Confila	Coutit

#### CVI\_UNF\_CIPHER\_HashFinal

【描述】

获取 hash 值。

【语法】

CVI S32 CVI UNF CIPHER HashFinal(CVI HANDLE hHashHandle, CVI U8 \*pu8OutputHash);

#### 【参数】

参数名称	描述	输入/输出	
hHashHandl	Hash 句柄	输入	
pu8OutputHash	输出的 hash 。	输出	采圳心
Ox	1 for	1	EOI
【返回值】	intiar	onfidential	
返回值	描述		
	18		

#### 【返回值】

	4 0 1	
返回值	描述	

confidential for Frame

Specifications are subject to change without notice

0 100	成功
<b>非</b> 0	参考错误码

### Confidential CVI\_UNF\_CIPHER\_GetRandomNumber

【描述】

生成随机数。

【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_GetRandomNumber(CVI\_U32

\*pu32RandomNumber);

#### 【参数】

参数名称	描述	输入/输出	
pu32RandomNumber	输出的随机数	输出	
【返回值】			•
返回值	描述		
O ************************************	成功		
非 0	参考错误码		
Conf.	dentia	Confidential	
UNF_CIPHER_GetTag			

#### 【返回值】

返回值	描述	THE T
0 深圳	成功	深圳
非 0	参考错误	玛

## Confidential CVI\_UNF\_CIPHER\_GetTag

【描述】

CCM/GCM 模式加解密后获取 TAG 值。

【语法】

CVI\_S32 CVI\_UNF\_CIPHER\_GetTag(CVI\_HANDLE hCipher, CVI\_U8 \*pstTag); 【参数】

参数名称	描述	输入/输出	
hCipher	CIPHER 句柄。	输入	
pstTag	TAG 值	输出	
【返回值】		TALL Y	<u> </u>
返回值	描述	£ #/////2	
0	成功	N	
非 0	参考错误码		
	Confident	confide	
	19		

#### 【返回值】

返回值	描述
0	成功
非0	参考错误码
	19

Confidential for 深圳随上



# CVI\_UNF\_CIPHER\_RsaPublicEncrypt 【描述】 Confidentia

使用 RSA 公钥加密一段明文。

【语法】

CVI S32

CVI\_UNF\_CIPHER\_RsaPublicEncrypt(CVI\_UNF\_CIPHER\_RSA\_PUB\_ENC\_S \*pstRsaEnc, CVI\_U8 \*pu8Input, CVI\_U32 u32InLen, CVI\_U8 \*pu8Output, CVI U32

CIPHER \*pu32OutLen);

#### 【参数】

	参数名称	描述	输入/输出	
	pstRsaEnc	公钥加密属性结构 体。	输入	
	pu8Input	待加密的数据。	输入	加州
	u32InLen	待加密的数据长度,	输入	深圳榧
	0,7	单位: byte。	1	601
	pu8Output	加密结果数据。	输出	
confide	pu32OutLen	加密结果数据长度,	输出	
		单位: byte	00	

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_RsaPrivateDecrypt

【描述】

使用 RSA 私钥解密一段密文。

【语法】

CVI\_S32

for深圳随着十 CVI\_UNF\_CIPHER\_RsaPrivateDecrypt(CVI\_UNF\_CIPHER\_RSA\_PRI\_ENC\_S \*pstRsaDec, CVI\_U8 \*pu8Input, CVI\_U32 u32InLen, CVI\_U8 \*pu8Output,



#### CVI\_U32

#### 【参数】

rations are subject to	change	without notice		
CVI_U32		深圳桥	魚	深圳雁
*pu32OutLen); 【参数】		tial for the	*;21	for 淡菜圳加
参数名称	<u> </u>	描述	输入/输出	
pstRsaEnc	Colli	私钥加密属性结构	输入 ( )	1
ļ		体。。		
pu8Input		待加密的数据。。	输入	
u32InLen		待加密的数据长度,	输入	
		单位: byte。		
pu8Output		加密结果数据。	输出	
pu32OutLen	-	加密结果数据长度,	输出	1
		单位: byte		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码
LINE CIDLED Deadublic	Hential for

# Confidential for CVI UNF CIPHER RsaPublicDecrypt

【描述】

使用 RSA 公钥解密一段密文。

【语法】

CVI S32

CVI\_UNF\_CIPHER\_RsaPrivateDecrypt(CVI\_UNF\_CIPHER\_RSA\_PUB\_ENC\_S \*pstRsaDec, CVI\_U8 \*pu8Input, CVI\_U32 u32InLen, CVI\_U8 \*pu8Output, CVI\_U32

\*pu32OutLen);

#### 【参数】

19 501			
参数名称	描述	输入/输出	
pstRsaDec	公钥解密属性结构体。	输入	深圳加
200	C (A)		c or
pu8Input	待解密的数据。	输入	70
u32InLen	待解密的数据长度,	输入	
$Co_{U_j}$		Cour	
	21		

Specifica	ations are subject to cr	iange without notice		
	<u> </u>		A.Y	
	深圳州	单位: byte。	/th	35 11/11/2
	pu8Output	解密结果数据。。	输出	Eoz
	pu32OutLen	解密结果数据长度,	输出	ntial
		单位: byte。	fid	Ell
	【返回值】	Colle	Com	
	<b>设回值</b>	##・#		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_RsaSign

【描述】

使用 RSA 私钥签名一段文本。

【语法】

al for \*\*\* thinket CVI\_S32 CVI\_UNF\_CIPHER\_RsaSign(CVI\_UNF\_CIPHER\_RSA\_SIGN\_S \*pstRsaSign, CVI\_U8

\*pu8InData, CVI\_U32 u32InDataLen, CVI\_U8 \*pu8HashData,CVI\_U8 \*pu8OutSign,

CVI\_U32 \*pu32OutSignLen);

#### 【参数】

参数名称	描述	输入/输出	
pstRsaSign	签名属性结构体。	输入	
pu8InData	待签名的数据, 如果	输入	
	pu8HashData 不为		
	空,则使		
	用 pu8HashData 进		
	行签名,该参数将被		
	忽略。		山頂
u32InDataLen	待签名的数据长度,	输入	深圳艇
or T	单位: byte。	4	Eoz 1
pu8HashData	待签名文本的 HASH	输入	
30	摘要,如果为空,则	fider	
$Co_{i_1}$		Corr	
	22		

Specifica	ations are subject to change	without notice		
	- A		X	A
	THE WAR	自动		THE HILL
	OZ IM	计算 pu8InData 的		tor the
		HASH 摘要进行签	+121	>
	C	名。	ci den	
	pu8OutSign	签名结果数据。	输出 ( )	
	pu32OutSignLen	签名结果数据长度,	输出	
		单位: byte。		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_RsaVerify

【描述】

使用 RSA 公钥签名验证一段文本。

《【语法】

for深圳随十 CVI\_S32 CVI\_UNF\_CIPHER\_RsaVerify(CVI\_UNF\_CIPHER\_RSA\_VERIFY\_S \*pstRsaVerify,CVI\_U8 \*pu8InData, CVI\_U32 u32InDataLen, CVI\_U8 \*pu8HashData,CVI U8 \*pu8InSign, CVI U32 u32InSignLen);

#### 【参数】

参数名称	描述	输入/输出	
pstRsaVerify	签名验证属性结构	输入	
	体。。		
pu8InData	待验证的数据, 如果	输入	
	pu8HashData 不为		
	空,则使		
	用 pu8HashData 进		
\ <u>\</u>	行验证,该参数将被	\ <u></u>	$\vee$
· WIE	忽略。		WHE T
u32InDataLen	待验证的数据长度,	輸入	深圳便
Ox	单位: byte	1	EOI
pu8HashData	待验证文本的的	输入	
30	HASH 摘要,如果为	of ide,	
	23		
	23		

Specific	ations are subject to	cnange	without notice		
	#1		Á	X	- A
	-12 All Miles		空,则自		- HILL .
	502 Ju		动计算 pu8InData 的		for the
	>		HASH 摘要进行验	121	<i>Y</i>
		C	证。	ciden	
	pu8InSign		待验证的签名数据。	输入 (0)	
	u32InSignLen		待验证的签名数据长	输入	
			度,单位:byte。。		

#### 【返回值】

返回值	描述
0	成功
非 0	参考错误码

#### CVI\_UNF\_CIPHER\_KladEncryptKey

【描述】

使用 KLAD 对透明密钥进行加密。

《【语法】

for深圳艇十 CV\_S32 CVI\_UNF\_CIPHER\_KladEncryptKey(CVI\_UNF\_CIPHER\_CA\_TYPE\_E enRootKey,

CVI\_UNF\_CIPHER\_KLAD\_TARGET\_E enTarget, CVI\_U8 \*pu8CleanKey, CVI\_U8\* pu8EcnryptKey, CVI\_U32 u32KeyLen);

#### 【参数】

参数名称	描述	输入/输出	
enRootKey	KLAD 根密钥选择,	输入	
	只能选择 EFUSE		
	Key₀		
enTarget	使用该密钥的模块。	输入	
pu8CleanKey	透明密钥	输入	_
pu8EcnryptKey	加密密钥。	输出	EOI 美洲種
u32KeyLen	密钥的长度,必须是	输入	**************************************
Or	16 整数倍。		EOI
【返回值】	100110	intia	•
返回值	描述	Confidential	
Con	24	Corr	

#### 【返回值】

返回值描述
-------

Confidential for 深圳雁十



Specifications are subject to change without notice

0 5 11/1/19	成功	爱圳椰
非 0	参考错误	码

### 2. 数据类型

#### 相关数据类型、数据结构定义如下:

- CVI\_HANDLE: 定义 CIPHER 的句柄类型。
- CVI UNF CIPHER WORK MODE E: 定义 CIPHER 工作模式。
- CVI UNF CIPHER ALG E: 定义 CIPHER 加密算法。
- CVI\_UNF\_CIPHER\_KEY\_LENGTH\_E: 定义 CIPHER 密钥长度。
- CVI UNF CIPHER BIT WIDTH E: 定义 CIPHER 加密位宽。
- ial for 深圳随 • CVI UNF CIPHER CTRL CHANGE FLAG S: 定义 CIPHER CCM 模式的信息 结

#### 构体。

- CVI UNF CIPHER CA TYPE E: 定义 CIPHER key 的来源。
- Confidential CVI\_UNF\_CIPHER\_KLAD\_TARGET\_E: 定义 Klad 产生的 Key 送达的目标选 择。
  - CVI UNF CIPHER TYPE E: 定义 CIPHER 加解密类型选择。
  - CVI UNF CIPHER ATTS S: 定义 CIPHER 加解密类型结构。
  - CVI UNF CIPHER CTRL S: 定义 CIPHER 控制信息结构体。
  - CVI\_UNF\_CIPHER\_CTRL\_AES\_S: AES 加密控制信息结构扩展。
  - CVI\_UNF\_CIPHER\_CTRL\_AES\_CCM\_GCM\_S: AES-CCM、AES-GCM 加密控 制

#### 信息结构。

- CVI\_UNF\_CIPHER\_CTRL\_DES\_S: DES 加密控制信息结构扩展。
- CVI\_UNF\_CIPHER\_CTRL\_3DES\_S: 3DES 加密控制信息结构。
- for深圳随中 • CVI\_UNF\_CIPHER\_CTRL\_EX\_S: 加密控制信息扩展结构作为算法的专用参数。
- - CVI UNF CIPHER HASH ATTS S: 定义 CIPHER 哈希算法初始化输入结构



- - CVI\_UNF\_CIPHER\_RSA\_PRI\_KEY\_S: 定义 RSA 私钥结构体。
  - CVI\_UNF\_CIPHER\_RSA\_PUB\_ENC\_S: 定义 RSA 公钥加解密算法参数结体。
  - CVI\_UNF\_CIPHER\_RSA\_PRI\_ENC\_S: 定义 RSA 私钥解密算法参数结构体。
  - CVI\_UNF\_CIPHER\_RSA\_SIGN\_S: 定义 RSA 签名算法参数输入结构体。
  - CVI UNF CIPHER RSA VERIFY S: 定义 RSA 签名验证算法参数输入结构体。
  - CIPHER IV CHANGE ONE PKG: CIPHER 为数据包设置向量时,仅更新一个 数

据包的IV。

CIPHER IV CHANGE ALL PKG: CIPHER 为数据包设置向量时, 更新所有数据 Confidential for Frime Confidential for 深圳種十 Confidential for TRHME

错误代码	宏定义	描述	
0x804D0001	CVI_ERR_CIPHER_NOT_INIT	设备未初始化	
0x804D0002	CVI_ERR_CIPHER_INVALID_HANDLE	Handle 号无效	
0x804D0003	CVI_ERR_CIPHER_INVALID_POINT	参数中有空指针	
0x804D0004	CVI_ERR_CIPHER_INVALID_PARA	无效参数	
0x804D0005	CVI_ERR_CIPHER_FAILED_INIT	初始化失败	
0x804D0006	CVI_ERR_CIPHER_FAILED_GETHANDLE	获取 handle 失败	
0x804D0007	CVI_ERR_CIPHER_FAILED_RELEASEHANDL	释放 handle 失败	
0x804D0008	CVI_ERR_CIPHER_FAILED_CONFIGAES	AES 配置无效	
	26	Court	

-	X		
0x804D0009	CVI_ERR_CIPHER_FAILED_CONFIGDES	DES 配置无效	
0x804D000A	CVI_ERR_CIPHER_FAILED_ENCRYPT	加密失败	
0x804D000B	CVI_ERR_CIPHER_FAILED_DECRYPT	解密失败	
0x804D000C	CVI_ERR_CIPHER_BUSY	忙状态	
0x804D000D	CVI_ERR_CIPHER_NO_AVAILABLE_RNG	没有可用的随机数	
0x804D000E	CVI_ERR_CIPHER_FAILED_MEM	内存申请错误	
0x804D000F	CVI_ERR_CIPHER_UNAVAILABLE	不可用	
0x804D0010	CVI_ERR_CIPHER_OVERFLOW	数据溢出	
0x804D0011	CVI_ERR_CIPHER_HARD_STATUS	硬件状态错误	
0x804D0012	CVI_ERR_CIPHER_TIMEOUT	等待超时	
0x804D0013	CVI_ERR_CIPHER_UNSUPPORTED	不支持的配置	
0x804D0014	CVI_ERR_CIPHER_REGISTER_IRQ	中断号无效	
0x804D0015	CVI_ERR_CIPHER_ILLEGAL_UUID	非法UUID	
0x804D0016	CVI_ERR_CIPHER_ILLEGAL_KEY	非法key	
0x804D0017	CVI_ERR_CIPHER_INVALID_ADDR	无效地址	
0x804D0018	CVI_ERR_CIPHER_INVALID_LENGTH	无效长度	
0x804D0019	CVI_ERR_CIPHER_ILLEGAL_DATA	无效数据	
0x804D001A	CVI_ERR_CIPHER_RSA_SIGN	RSA 签名失败	
0x804D001B	CVI_ERR_CIPHER_RSA_VERIFY	RSA 校验失败	
0x804D001E	CVI_ERR_CIPHER_RSA_CRYPT_FAILED	RSA 加解密失败	
-1	CVI_FAILURE	操作失败	
0x004D0001	CVI_LOG_ERR_MEM	内存操作失败	
0x004D0002	CVI_LOG_ERR_SEM	Semaphore 操作失	
0x004D0003	CVI_LOG_ERR_FILE	文件操作失败	
	4X		
0x004D0004	CVI_LOG_ERR_LOCK	锁操作失败	
0x004D0005	CVI_LOG_ERR_PARAM	参数无效	
0x004D0006	CVI_LOG_ERR_TIMER	计时器错误	
0x004D0007	CVI_LOG_ERR_THREAD	线程失败	



	m× m×	1	人類人
0x004D0008	CVI_LOG_ERR_TIMEOUT	超时	深圳州
0x004D0009	CVI_LOG_ERR_DEVICE	Device 操作失败	for深圳随
0x004D0010	CVI_LOG_ERR_STATUS	状态出错	, L
0x004D0011	CVI_LOG_ERR_IOCTRL	IO 操作失败	
0x004D0012	CVI_LOG_ERR_INUSE	资源使用中	
0x004D0013	CVI_LOG_ERR_EXIST	退出失败	
0x004D0014	CVI_LOG_ERR_NOEXIST	资源未退出	
0x004D0015	CVI_LOG_ERR_UNSUPPORTED	不支持	
0x004D0016	CVI_LOG_ERR_UNAVAILABLE	不可用	
0x004D0017	CVI_LOG_ERR_UNINITED	未初始化	
0x004D0018	CVI_LOG_ERR_DATABASE	数据库出错	
0x004D0019	CVI_LOG_ERR_OVERFLOW	溢出	
0x004D0020	CVI_LOG_ERR_EXTERNAL	外部出错	
0x004D0021	CVI_LOG_ERR_UNKNOWNED	位置错误	for 深圳随
0x004D0022	CVI_LOG_ERR_FLASH	Flash 操作失败	1 60,
0x004D0023	CVI_LOG_ERR_ILLEGAL_IMAGE	非法镜像	
0x004D0024	CVI_LOG_ERR_ILLEGAL_UUID	非法UUID	
0x004D0025	CVI_LOG_ERR_NOPERMISSION	操作不允许	