基于 CIU98_B V2 的 T-BOX SE[V3160-1.1] 应用参考设计说明书

V1.0

北京中电华大电子设计有限责任公司
CEC Huada Electronic Design Co.,Ltd

2021 年 06 月

声　明

变更记录

版本	修改描述	日期
V1.0	初稿	2021-06-22

目 录

1. 目的 1
2. 适用范围 1
3. 参考资料 1
4. 名词解释 1
5. 概述 1
6. 参考设计 2
6.1. 个人化 2
6.1.1. 文件结构 3
6.1.2. 密钥结构 3
6.2. 管理功能 6
6.2.1. 更新管理密钥 6
6.2.2. 更新应用密钥 6
6.2.3. 装载 SE ID 7
6.3. 应用功能 7
6.3.1. 对称算法 7
6.3.2. 非对称算法 7
6.3.3. 哈希算法 7
6.3.4. 文件读写 8
6.3.5. 临时密钥操作 8
6.3.6. 产生密钥对 8
6.3.7. 导出公钥 8
6.3.8. 读取 SE ID 8
6.3.9. 获取 SE 信息 9
6.3.10. 功耗管理 9

1. 目的

本文档介绍了基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]应用实例，指导用户后续的发行及使用工作。

本文档所介绍的 SE 应用参考下的个人化、管理功能和应用功能均有对应的脚本，作为文档的附件一并提供。

2. 适用范围

本文档适用于应用工程师（ESAE）、技术支持工程师(ESTSE)。

3. 参考资料

- 《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》V1.0

4. 名词解释

- SE Security Element
  安全单元。
- 个人化
  文件创建及密钥灌装。

5. 概述

本文档是基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]的应用参考，详细描述了该款 SE 的个人化，包括个人化流程、文件结构和密钥结构，以及管理功能和应用功能，并提供了相应脚本，作为产品包的一部分供用户使用。

6. 参考设计

参考设计包括 SE 的个人化、管理功能和应用功能，其中个人化主要为文件创建和密钥灌装，管理功能包括更新管理密钥、导入应用密钥和装载 SE ID，应用功能包括对称算法、非对称算法、哈希算法、临时密钥操作、文件读写和读取 SE ID 等应用功能。

6.1. 个人化

个人化参考脚本为《个人化参考设计脚本.txt》。

典型的个人化流程如下：

1. 复位
2. 认证设备主控密钥
3. 清除文件
4. 创建 SE 应用目录‘DDF1’
5. 装载管理密钥
6. 建立二进制文件‘0005’
7. 建立二进制文件‘0006’
8. 建立二进制文件‘0007’
9. 建立二进制 SE 证书文件‘0008’
10. 建立二进制 CA 证书文件‘0009’
11. 写入 SE ID
12. 装载 3DES 对称算法密钥
13. 装载 AES 对称算法密钥
14. 装载 SM4 对称算法密钥
15. 装载 ECC 非对称算法密钥
16. 装载 RSA 非对称算法密钥
17. 装载 SM2 非对称算法密钥

以下给出了个人化中参考的文件结构和密钥结构。

6.1.1. 文件结构

在符合 SE 应用基本要求的前提下，可根据特定需求来扩展自定义的文件结构，供预留使用。下面列举一个推荐的文件结构信息，如图 6.1 所示，后续操作按此结构介绍。

1) 文件结构图

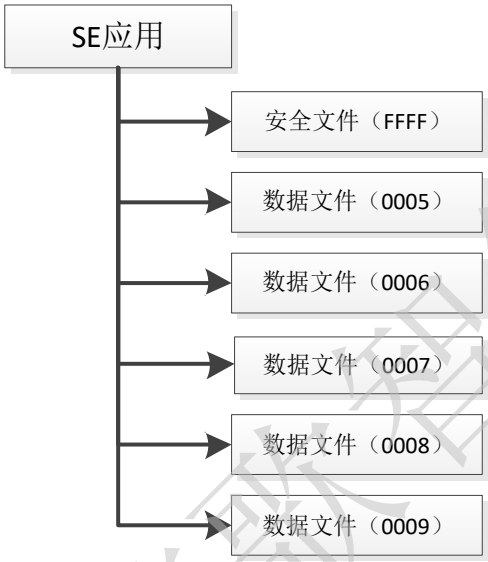

图 6.1 文件结构图

2) 文件结构说明

文件标识	文件内容	文件大小	读属性	写属性	说明
‘FFFF’	安全文件	——	无	管理员权限	内部文件，不可操作，支持的 KID 范围为 00-EF，写入受控
‘0005’	数据文件	1024 B	无	无	非敏感类或临时数据，读写自由
‘0006’	数据文件	1024 B	无	管理员权限	敏感类数据，写入受控
‘0007’	数据文件	1024 B	管理员权限	管理员权限	敏感类数据，读写受控
‘0008’	数据文件	2048 B	无	用户权限	SE 证书文件
‘0009’	数据文件	2048 B	无	用户权限	CA 证书文件

6.1.2. 密钥结构

1) 管理密钥

设备主控密钥、管理员 PIN、用户 PIN 用于获取权限，传输密钥用于安全报文传输。

密钥名称	密钥用途	密钥 ID	密钥值
设备主控密钥	—	—	404142434445464748494A4B4C4D4E4F
管理员 PIN	00	00	123456789ABCDEF0123456789ABCDEF0

用户 PIN	00	01	112233445566
传输密钥	01	02	404142434445464748494A4B4C4D4E4F

2) 应用密钥

a) 对称密钥

算法类型	密钥名称	密钥用途	密钥 ID	密钥值
3DES128	3DES_KEY	02	03	00000000000000000000000000000000
AES128	AES128_KEY	02	04	00000000000000000000000000000000
SM4	SM4_KEY	02	06	00000000000000000000000000000000

b) 非对称密钥

算法类型	密钥分量	密钥用途	密钥 ID	密钥值
ECC256	ECC256_pub	02	09	D17ED15EDFFFFBC6DB023E1F4E4B9A45C590A816F8CAE301633940E483791728C85E5C328BC059F7A30496B846B5932E7E3E1D34AB53B3CBFF1D98954EFDF511
	ECC256_pri	02	0A	160B55FF3B18EEAEF8F0789B5B0912269EBDE19D41079D87B27522F345723EA9
RSA1024 CRT	E	02	0B	00010001
	RSA1024_pub	02	0B	CE0BA793E1271566F863C81CC2276BE17B3A581CBDE097536BD37EF6C61E30C36D4E0808E47243B9997D6FAEA664B00EEF7873F5F247263E835F1C9DB9EFA9AFFCDE658B3F72966B056D27A09C2F41D8B02A3A5697D2B40BEDA4C8BA750A80FD68521DB1ED441B94DB2A5B4E1BBCD44C64D6D2917B423AA91F0C146788D69055
	RSA1024_P	02	0C	FEE8AC71C6526090A9835EA1C0A4DDA6BC7157A77F9B9D614472C665A9CEC2C257A9D775C2BDA170DE62B9EA6278C3B8A9C9D641DB4A895384747576A9608DD1
	RSA1024_Q			CEED6FE2C2E3454CD9A984784E4C64B68DAEB7E8E0A6A34EE2B86563A7E1C894E7D5889FCBBA49D5A35367CE735A70C4467DEEA5DBD3D2BA61D1E68492BDA745
	RSA1024_DP			BE6C96960FEF6E0FE3722DF96BEE3D5ED79B5C3DD6882B93840CB1C5348B2ED6FBA1F741138F91D0BD70C72E1F0DD438592E5C8EAA010E81838B744C86CF8861
	RSA1024_DQ			56FC9D5238170E24D6435ABAB03F90FEE4E493

				CF43D10949BA294605F4A70789014454A0C825D1B00B6E9E6EBD3341C060D9C39ED9A05C2F99BB812A2DFDA7F9
	RSA1024_INVQ			456FE77BBD2493BAD9D767C9B36A303AD30CED3703095A909FA0FBBA3FC1B0B6046F05E551D8598F1C690D678D743B985E7029CD6D0E1A3975C7314829C2ED68
RSA2048 CRT	E	02	0D	00010001
	RSA2048_pub			B25AE3DFDDF5C244817320AAC543D8DF6546E41ECFFC641EE22B4738315428A1F2E5FAE7EAF419FE36DF948F0AFD042D675E750C1FF712CD80DE7C5861C8D1594A561B0741716824222631F694E318A0400E9ACE270838B3A1EE067C9147C6CD14C8F0419FB12742EB0DE25B7D2F59A7270C31EA04BC9CF93CD6D4B8511A8913DA9BF951F0E29915B53C395658E9BA74A3B529D6C884171E3ADCE5C25C56678C5512C3171C08939CDDDCB71B4382CDC9C32295C4133B236AD1E5DC4E41C6B90CB52C8AC6AD3019E5F0CF867C67C96F1955CAF07921984BAA6EC97B669526CD4D1974D7A20263E5442E770DA9825AB5232E0053895F6DB82DAA5E417ECE67F959
	RSA2048_P			ED4F60E9BEC7D190988E92BC8248434EC3AFE678C568E57F4C4D6289BC53B9648990E3D2C3B34C4A47997B619E7054CBCB6DC6EF777D6946E0A0D2528D99A5B4815796CC574268838DC98979CE52D478B05D567DB587905E54708C697DACDED1DAD959D2C56AE3AD69ECA6D3577367C25A5549577E527545B5D894B755B3D46F
	RSA2048_Q			C066DDC078545BB1567FB5C492974F4C78B07488BB7572D391BA5E834191B4B28DE0945470A095C7645AC3E14DC4836FA89A4BAA7766CC9B4C57E67F71C6C3BFAAC57DDF82A5D4996BD9D8C66DC3E26A759BA38C5191A5E2904BBDE3988CD1AA71768EAE5FB0CA4E8C71CD9D539AD7D3BB6667B6C0C862809956806E9F91C2B7
	RSA2048_DP			522AFDFF715376B87E5A3F6C8E1FBF4E726B617DC7BCBE5A096D720506F46668ED4901D964719CA4CB8DD52EC3D1594B07310784BAF6ED90E10E4E44CF4AB8197BFF7BF35CF35D84CF7F4CDEA416020397ED79992555BF232A519E0C98BB569B8B0F5F0E9FD496E8E098545B31188080C70E68CAA6AE9E7478B67927D1C0E679
	RSA2048_DQ			B83785A8CC4D910189DD7B8F3C002E07FD228

				E61808322AF59BF84D0CDCE11A2485FB805E5548C343E6CFD51D2A10E6BB196124EA446442F89783C14D83E449C5689034D270D5A328F6624BD50C99616F28653A07D5523EC7AD65A78F94E134DCB97856385F182B2949C3E0F9DC60B520A0331D8745B289D12B41502563C3C9F
	RSA2048_INVQ			48D0E05C4F49E480C09BDF0AEB712DE24556F2ECA76F1FEA2E33DBAAE63AEFD4E5479C31212F6648A63A81821F13C5F5C88F68FCC37B8D4653EFD8A3F2109DE6EBFBEA00CB29557A64C6730CB47FF0CEBBE6738EBB5FD455EE159E4BA41583AF981CAE7BF2A72F36794D705587155D85E75E8D5013A2A2A08316999880CE2A92
SM2	SM2_pub	02	0F	160E12897DF4EDB61DD812FEB96748FBD3CCF4FFE26AA6F6DB9540AF49C942324A7DAD08BB9A459531694BEB20AA489D6649975E1BFCF8C4741B78B4B223007F
	SM2_pri			81EB26E941BB5AF16DF116495F90695272AE2CD63D6C4AE1678418BE48230029

6.2. 管理功能

6.2.1. 更新管理密钥

个人化流程完成之后，可进行更新管理密钥操作，对应的参考脚本为《更新管理密钥.txt》。

更新管理密钥通过 WRITE KEY 命令、CHANGE PIN 更新，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》。

6.2.2. 更新应用密钥

个人化流程完成之后，可进行更新应用密钥操作，对应的参考脚本为《更新应用密钥.txt》。

更新应用密钥通过 IIMPORT KEY 命令更新，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》。

更新应用密钥之前需进行管理员 PIN 验证，以获得应用密钥更新权限。

6.2.3. 装载 SE ID

个人化流程完成之后，可进行 SE ID 装载操作，对应的参考脚本为《装载 SEID.txt》。

装载 SE ID 通过 WRITE SEID 命令装载，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》。

无论是否已经存在 SE ID 都允许装载或更新 SEID，装载 SE ID 需要获取设备主控密钥权限。

6.3. 应用功能

本部分主要介绍对称算法、非对称算法、哈希算法、文件读写、临时密钥操作、产生密钥对、导出公钥、读取 SE ID、获取 SE 信息及功耗管理等的应用功能，此部分的使用应在 SE 完成个人化之后进行。

6.3.1. 对称算法

对称算法包括 3DES、AES 和 SM4，由 CIPHER DATA 命令实现加密、解密、MAC 计算和 MAC 校验，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《对称算法 3DES.txt》、《对称算法 AES.txt》和《对称算法 SM4.txt》。

6.3.2. 非对称算法

非对称算法包括 ECC、RSA 和 SM2，由 PKI ENCIPHER/PKI DECIPHER/COMPUTE SIGNATURE/VERIFY SIGNATURE 命令实现加密、解密、签名和验签，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《非对称算法 ECC.txt》、《非对称算法 RSA.txt》和《非对称算法 SM2.txt》。

6.3.3. 哈希算法

哈希算法包括 SHA 系列和 SM3，由 HASH OPERATION 命令实现哈希计算，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》。其中 SHA 系列算法以 SHA1 和 SHA256 为例。对应的参考脚本为《哈希算法 SHA1.txt》、《哈希算法 SHA256.txt》和《哈希算法 SM3.txt》。

6.3.4. 文件读写

文件写由 UPDATE BINARY 命令实现，文件读由 READ BINARY 命令实现，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《文件读写.txt》。

6.3.5. 临时密钥操作

临时密钥操作包括导入、导出、删除、协商、产生及计算。其中删除由 DELETE KEY 命令实现，导入由 IMPORT KEY 命令实现，导出由 EXPORT KEY 命令实现，产生由 GENERATE KEY 命令实现，协商由 GENERATE SHARED KEY 命令实现，计算由 CIPHER DATA 命令，或 PKI ENCIPHER/PKI DECIPHER/COMPUTE SIGNATURE/VERIFY SIGNATURE 命令实现实现。具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《临时密钥操作.txt》。

6.3.6. 产生密钥对

产生密钥对由 GENERATE KEY 命令实现，可以内部生成密钥对同时返回公钥，也可以更新已存在的密钥对。具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《产生密钥对.txt》

6.3.7. 导出公钥

导出公钥由 EXPORT KEY 命令实现，仅用于导出非对称密钥的公钥。具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《导出公钥.txt》。

6.3.8. 读取 SE ID

读取 SEID 由 GET SEID 命令实现，需装载 SEID 后执行此项操作，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《读取 SEID.txt》。

6.3.9. 获取 SE 信息

获取 SE 信息由 QUERY 实现，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《获取 SE 信息.txt》。

6.3.10. 功耗管理

功耗管理由 ENTER LOW POWER 实现，具体参数参见《基于 CIU98_B V2 的 T-BOX SE[V3160-1.1]用户使用手册》，对应的参考脚本为《功耗管理.txt》。