基于 CIU98_B V2 的 T-BOX SE[V3160-1.1] 文件结构说明

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 12 月

声　明

变更记录

版本	修改描述	日期
V1.0	初稿	2021-12-13

目 录

1. 产品状态

- SPI 接口，时钟频率最高 15MHz，ATR：3B17008100316000401D；
- I2C 接口，通讯速率最高 400kbps，ATR：3B17118100316000401D；
- SE 的生命周期处于应用状态。

2. 文件结构

1) 文件结构图

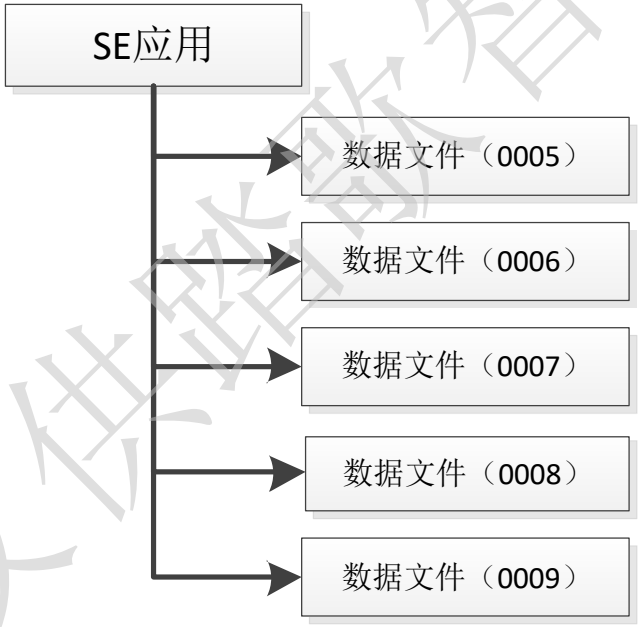

图 2.1 文件结构图

2) 文件结构说明

文件标识	文件内容	文件大小	读权限	写权限	说明
‘0005’	数据文件	1024 B	无	无	读写自由
‘0006’	数据文件	1024 B	无	管理员权限	写入受控，可用于存储敏感数据
‘0007’	数据文件	1024 B	管理员权限	管理员权限	读写受控，可用于存储敏感数据
‘0008’	数据文件	2048 B	无	管理员权限	写入受控，可用于存储 SE 证书文件
‘0009’	数据文件	2048 B	无	管理员权限	写入受控，可用于存储 CA 证书文件

3. 密钥结构

1) 管理密钥

密钥名称	密钥用途	密钥 ID	初始密钥值	说明
设备主控密钥	—	—	40414243444546474849 4A4B4C4D4E4F	用于应用的创建和删除，本产品中已创建默选应用“SE 应用”。
管理员 PIN	00	00	123456789ABCDEF0123456789ABCDEF0	用于获取管理员权限，可对 0006~0009 文件进行读写操作； 用于管理员 PIN、传输密钥和应用密钥的创建和更新，及应用密钥的删除； 也可用于“SE 应用”下文件的创建和删除。
传输密钥	01	02	40414243444546474849 4A4B4C4D4E4F	用于对 SE 和 MCU 之间传输的数据进行加密保护。

上述 3 条密钥需要更新后使用，否则会遗留安全隐患。

2) 应用密钥

a) 对称密钥

算法类型	密钥长度	密钥用途	密钥 ID	初始密钥值
3DES	128 位	02	03	00000000000000000000000000000000
AES	128 位	02	04	00000000000000000000000000000000
SM4	128 位	02	06	00000000000000000000000000000000

b) 非对称密钥

算法类型	密钥分量	密钥用途	密钥 ID	初始密钥值
ECC256	ECC 公钥	02	09	D17ED15EDFFFFBC6DB023E1F4E4B9A45C590 A816F8CAE301633940E483791728C85E5C328BC 059F7A30496B846B5932E7E3E1D34AB53B3CBF F1D98954EFDF511
	ECC 私钥			160B55FF3B18EEAEF8F0789B5B0912269EBDE1 9D41079D87B27522F345723EA9
RSA1024	E	02	0B	00010001

CRT	RSA 公钥			CE0BA793E1271566F863C81CC2276BE17B3A581CBDE097536BD37EF6C61E30C36D4E0808E47243B9997D6FAEA664B00EEF7873F5F247263E835F1C9DB9EFA9AFFCDE658B3F72966B056D27A09C2F41D8B02A3A5697D2B40BEDA4C8BA750A80FD68521DB1ED441B94DB2A5B4E1BBCD44C64D6D2917B423AA91F0C146788D69055
	RSA 私钥 P			FEE8AC71C6526090A9835EA1C0A4DDA6BC7157A77F9B9D614472C665A9CEC2C257A9D775C2BDA170DE62B9EA6278C3B8A9C9D641DB4A895384747576A9608DD1
	RSA 私钥 Q			CEED6FE2C2E3454CD9A984784E4C64B68DAEB7E8E0A6A34EE2B86563A7E1C894E7D5889FCBBA49D5A35367CE735A70C4467DEEA5DBD3D2BA61D1E68492BDA745
	RSA 私钥 DP			BE6C96960FEF6E0FE3722DF96BEE3D5ED79B5C3DD6882B93840CB1C5348B2ED6FBA1F741138F91D0BD70C72E1F0DD438592E5C8EAA010E81838B744C86CF8861
	RSA 私钥 DQ			56FC9D5238170E24D6435ABAB03F90FEE4E493CF43D10949BA294605F4A70789014454A0C825D1B00B6E9E6EBD3341C060D9C39ED9A05C2F99BB812A2DFDA7F9
	RSA 私钥 INVQ			456FE77BBD2493BAD9D767C9B36A303AD30CED3703095A909FA0FBBA3FC1B0B6046F05E551D8598F1C690D678D743B985E7029CD6D0E1A3975C7314829C2ED68
RSA2048 CRT	E	02	0D	00010001
	RSA 公钥			B25AE3DFDDF5C244817320AAC543D8DF6546E41ECFFC641EE22B4738315428A1F2E5FAE7EAF419FE36DF948F0AFD042D675E750C1FF712CD80DE7C5861C8D1594A561B0741716824222631F694E318A0400E9ACE270838B3A1EE067C9147C6CD14C8F0419FB12742EB0DE25B7D2F59A7270C31EA04BC9CF93CD6D4B8511A8913DA9BF951F0E29915B53C395658E9BA74A3B529D6C884171E3ADCE5C25C56678C5512C3171C08939CDDDCB71B4382CDC9C32295C4133B236AD1E5DC4E41C6B90CB52C8AC6AD3019E5F0CF867C67C96F1955CAF07921984BAA6EC97B669526CD4D1974D7A20263E5442E770DA9825AB5232E0053895F6DB82DAA5E417ECE67F959
	RSA 私钥 P			ED4F60E9BEC7D190988E92BC8248434EC3AFE678C568E57F4C4D6289BC53B9648990E3D2C3B

				34C4A47997B619E7054CBCB6DC6EF777D6946E 0A0D2528D99A5B4815796CC574268838DC9897 9CE52D478B05D567DB587905E54708C697DAC DED1DAD959D2C56AE3AD69ECA6D3577367C 25A5549577E527545B5D894B755B3D46F
	RSA 私钥 Q			C066DDC078545BB1567FB5C492974F4C78B074 88BB7572D391BA5E834191B4B28DE0945470A0 95C7645AC3E14DC4836FA89A4BAA7766CC9B4 C57E67F71C6C3BFAAC57DDF82A5D4996BD9D 8C66DC3E26A759BA38C5191A5E2904BBDE398 8CD1AA71768EAE5FB0CA4E8C71CD9D539AD7 D3BB6667B6C0C862809956806E9F91C2B7
	RSA 私钥 DP			522AFDFF715376B87E5A3F6C8E1FBF4E726B61 7DC7BCBE5A096D720506F46668ED4901D96471 9CA4CB8DD52EC3D1594B07310784BAF6ED90E 10E4E44CF4AB8197BFF7BF35CF35D84CF7F4C DEA416020397ED79992555BF232A519E0C98BB 569B8B0F5F0E9FD496E8E098545B31188080C70 E68CAA6AE9E7478B67927D1C0E679
	RSA 私钥 DQ			B83785A8CC4D910189DD7B8F3C002E07FD228 E61808322AF59BF84D0CDCE11A2485FB805E55 48C343E6CFD51D2A10E6BB196124EA446442F8 9783C14D83E449C5689034D270D5A328F6624B D50C99616F28653A07D5523EC7AD65A78F94E1 34DCB97856385F182B2949C3E0F9DC60B520A0 331D8745B289D12B41502563C3C9F
	RSA 私钥 INVQ			48D0E05C4F49E480C09BDF0AEB712DE24556F2 ECA76F1FEA2E33DBAAE63AEFD4E5479C3121 2F6648A63A81821F13C5F5C88F68FCC37B8D46 53EFD8A3F2109DE6EBFBEA00CB29557A64C67 30CB47FF0CEBBE6738EBB5FD455EE159E4BA4 1583AF981CAE7BF2A72F36794D705587155D85 E75E8D5013A2A2A08316999880CE2A92
SM2	SM2 公钥	02	0F	160E12897DF4EDB61DD812FEB96748FBD3CCF 4FFE26AA6F6DB9540AF49C942324A7DAD08B B9A459531694BEB20AA489D6649975E1BFCF8C 4741B78B4B223007F
	SM2 私钥			81EB26E941BB5AF16DF116495F90695272AE2C D63D6C4AE1678418BE48230029

4. SEID

1) SEID 长度为 1~255 字节；
2) SEID 出厂时未写入，由客户自行写入；
3) 在认证设备主控密钥后，SEID 可通过 WRITE SEID 命令写入或修改。