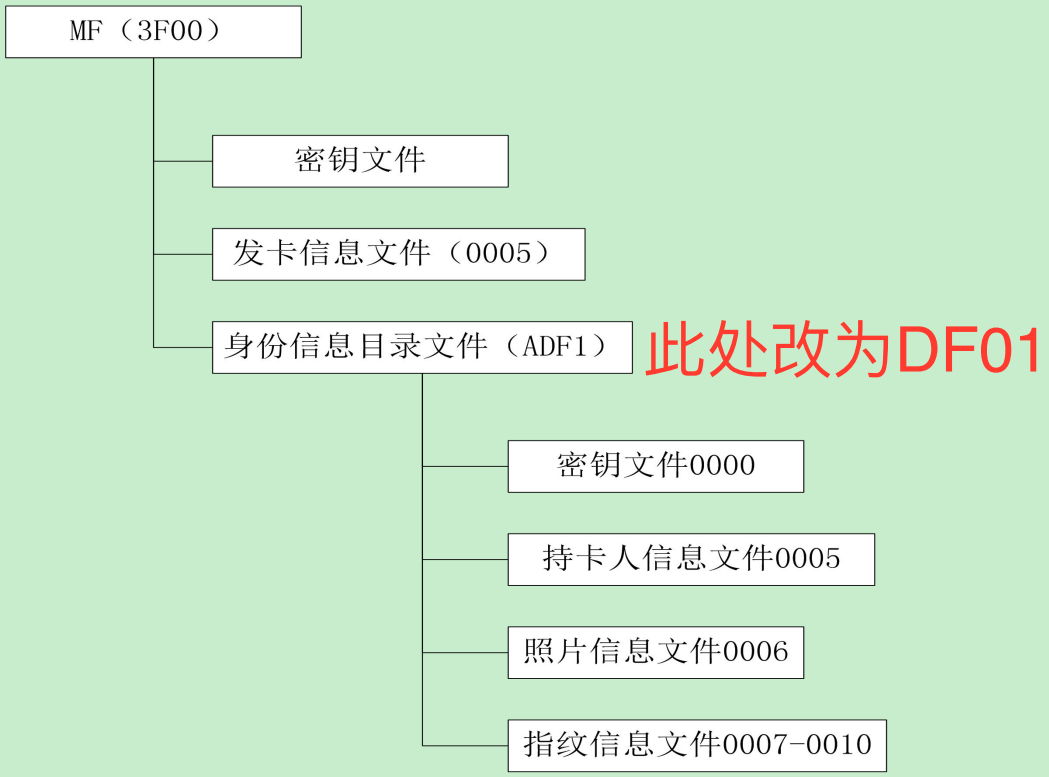
伊朗项目卡结构

版本	时间	作者	注释
V0.1	2017-6-14	Shsun	初始版本，对卡结构进行原始规划

目录：

卡结构框图：



MF（3F00）

MF 下文件信息

文件名称	文件类型	标识符	大小	权限设计	
MF	目录文件	3F00		建权：主控	擦权：主控+主控线路保护
密钥文件	密钥文件	0000	50B	读：禁止	更新：DCCK 加密+DCCK 线路保护
制卡信息文件	二进制文件	0005	2*0x17B	读权：自由	写权：DCMK 线路保护

MF 密钥信息

密钥名称	类型	索引
卡片主控 DCCK	主控密钥（39）	0
卡片维护 DCMK	维护密钥（36）	0

ADF1 身份信息文件

ADF1 目录下文件信息

文件名称	文件类型	标识符	大小	权限设计	
密钥文件	密钥文件	0000	5*0x17B	读权：禁止	更新：DCCK 加密+DCCK 线路保护
持卡人信息文件	二进制文件	0005	64B	读权： DACK1 外部认证	写权： DACK2 外部认证
照片信息文件	二进制文件	0006	2048B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 1	二进制文件	0007	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 2	二进制文件	0008	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 3	二进制文件	0009	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 4	二进制文件	000A	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 5	二进制文件	000B	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 6	二进制文件	000C	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 7	二进制文件	000D	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 8	二进制文件	000E	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 9	二进制文件	000F	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证
指纹信息文件 10	二进制文件	0010	1024B	读权： DACK4 外部认证	写权： DACK3 外部认证

ADF1 密钥信息

密钥名称	类型	索引
应用主控 DACK0	主控密钥（39）	0
应用主控 DACK1	外部认证密钥（39）	1
应用主控 DACK2	外部认证密钥（39）	2
应用主控 DACK3	外部认证密钥（39）	3
应用主控 DACK4	外部认证密钥（39）	4

关键字说明：

MAC：按照 PBOC 规范进行的 MAC 计算

DATA_ENC:数据加密计算，数据串最前面补数据长度，后补 80 00...等到 8 字节整数倍作为源数据，使用密钥进行加密运算。

密钥更新流程：

00 84 0000 08

84D4 39 00 1C DATA_ENC(39 00 AAFF33 DCCK_NEW,DCCK)

MAC(84D4 39 00 1C DATA_ENC(3900AAFF33 DCCK_NEW,DCCK),DCCK,RNG)

其中，39 为密钥类型；00 为密钥索引；

制卡信息文件更新流程：

获取随机数 RNG：0084000008

更新 0005 文件：

00D68500 24 000000000000000000000000000000000000000000000000000000000000000000

MAC(00D68500 24 000000000000000000000000000000000000000000000000000000000000 0000 00 ，DCMK，RNG)

制卡信息文件读取流程：

读取信息：00B0850020

持卡人信息更新流程：

获取随机数 RNG：0084000008

外部认证 DACK1：0082 0001 08 ENC（RNG，DACK2）

更新文件：00D685 00 40 DATA[0-64]

持卡人信息读取流程：

获取随机数 RNG：0084000008

外部认证 DACK1：0082 0001 08 ENC（RNG，DACK1）

读取文件：00B085 00 40

照片信息/指纹信息更新流程：

获取随机数 RNG：0084000008

外部认证 DACK3：0082 0001 08 ENC（RNG，DACK3）

更新文件：（单次更新 200 字节，直到 2048/1024 字节更新完毕）

00A4 00 00 02 0006 /[0007-0010]

00D6 00 00 C8 DATA[0-199]

00D6 00 C8 C8 DATA[200-399]

00D6 01 90 C8 DATA[400-599]

…… …

照片信息/指纹信息读取流程：

获取随机数 RNG：0084000008

外部认证 DACK4：0082 0001 08 ENC（RNG，DACK4）

更新文件：（单次 读取 200 字节，直到 2048/1024 字节读取完毕）

00A4 00 00 02 0006 /[0007-0010]

00B0 00 00 C8 DATA[0-199]

00B0 00 C8 C8 DATA[200-399]

00B0 01 90 C8 DATA[400-599]

…… …