Mifare DESFire（MF3 IC D40/D41,本文以 D40 为例）遵守 14443 TypeA 协议，卡内的数据以文件形式存储，所以有人认为它是准 CPU 卡，主要用于安全性要求较高的非接触式领域。

与普通 MF1 S50 不同，DESFire 的数据传输速率不仅支持最基本的 106Kbps，还支持 212Kbps 和 424Kbps；其数据传送的加密方法也不再使用已经被破解的 Crypto1 加密流，而是使用更为安全的 DES/3DES、AES 加密，至少 DES/3DES 和 AES 已经经过了多年的公开检验，至今还没有被破解。

DESFire 的全球唯一序列号是 7 字节，支持 ISO14443-4 和 ISO7816 的部分协议。7 字节的序列号要使用两个防冲突循环才能读出，第一轮防冲突循环卡片返回层级代码 0x88， UID 的前 3 个字节 SN0-SN2 和校验码 BCC0，第二轮防冲突循环返回 UID 的后 4 个字节 SN3-SN6 和校验码 BCC1，SN0 为制造商的 ID 号，NXP 产品固定为 16 进制的 04H.

DESFire 有 4K 字节的非易失存储空间，典型的写时间为 2ms（1ms 擦除，1ms 编程)。存储空间的组织采用柔性文件系统，D40 卡上可同时最多支持 28 种应用,每种应用用一个 3 字节的应用标识符（AID）表示，每种应用可以设置序号为 0-13 的最多 14 组不同的密码，每种应用下可建立最多 16 个文件.

卡片支持 5 种不同的文件类型，每种类型使用一个字节的类型编码来表示。文件类型及其编码如下:

文件类型	类型编码
标准数据文件	0x00
备份数据文件	0x01
带有备份的值文件	0x02
带有备份的线性记录文	0x03
带有备份的循环记录文件	0x04

每种应用与读写器之间的通讯加密等级根据安全性不同分为 3 类，使用一个字节的通讯设置码来表示。通讯设置码的各个 bit 代表的意义如下表所示：

通讯模式	Bit7-bit2	Bit1	Bit0
明文通讯	RFU=0	忽略	0
具有 DES/3DES MAC 校验的明文通讯	RFU=0	0	1
完全 DES/3DES 密文通讯	RFU=0	1	1

明文模式最简单，就是直接传送没有加密的真值，一旦被截获，黑客看到的就是真实信息；

带有 MAC 校验的明文传输也好不到哪里去，它是把要传送的明文用 CBC 模式进行 DES/3DES 加密，把最后一步的 8 字节加密输出结果中的前 4 字节称为 MAC 校验，加在要传送的明文后面，前面的明文还是明文，只不过加了个校验防止出错而已；

只有第三种完全 DES/3DES 密文通讯才对得起“DESFire”这个名字，这是真正的加密通讯。所有要传送的密文先用 CRC16 进行校验，然后明文连同 CRC16 校验作为一个整体使用 CBC 模式的 DES/3DES 加密，传送的是加密后的密文。黑客即使截获了也看不懂，前提是不知道 DES 密码。

前面叙述时经常用 DES/3DES 这个组合，那到底是 DES 还是 3DES 呢，二者的运算量和加密强度可是有天壤之别啊！这一点 DESFire 卡片采用了自动识别的方法。DES 和 3DES 密钥的长度都是 16 字节，如果前 8 字节与后 8 字节相同，则自动被作为 DES 运算；反之，如果前 8 字节与后 8 字节不同，则自动被作为 3DES 运算。

DES 密钥举例：0x00 11 22 33 44 55 66 77 00 11 22 33 44 55 66 77

0x00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

3DES 密钥举例：0x00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

0x00 11 22 33 44 55 66 77 00 00 00 00 00 00 01 00

0x00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00

D40 卡片的默认出厂设置为密钥全 0，单 DES 操作。

DESFire 卡片可以为应用中的文件设置不同的读写权限，读写权限的意思就是读或写文件时是否需要验证密码，以及验证哪一组密码。读写权限使用 2 个字节的编码来表示，2 个字节共 16 个 bit，每 4 个 bit 表示一种权限类型：

15 12 11 8 7 4 3 0

读文件 要验证的密码	写文件 要验证的密码	读和写文件 要验证的密码	修改文件的读写权限 要验证的密码

前面说了，每种应用可以有编号为 0-13 的最多 14 组不同的密码，而 4 位二进制数可以表示 0-15 共 16 种组合。当 4 位权限码的值为 0-13 时，表示执行相应的读写操作要验证权限码的值指向的一组密码；当权限码的值为 14 时，表示不用验证任何密码可直接读写；权限码的值为 15 时表示冻结，就是不论什么条件也不让读写了。

DESFire 的卡片命令可以分为 6 大类：

(1)ISO14443-3 命令

(2)ISO14443-4 命令

(3)安全相关命令

(4)卡片级命令

(5)应用层命令

(6)数据操作命令

3 次握手认证并生成临时的通讯密钥在通讯技术中的应用非常普遍，Mifare Desfire 也使用了这种成熟的认证加密方法。Desfire 在卡片数据传输前使用 DES 或 3DES 进行 3 次握手认证，认证成功一方面表明卡片和读写器双方是可以相互信任的，同时为双方之后的数据传送提供了一组临时使用的段密码进行加密保护。

DES/3DES 的基本运算包括加密和解密，Desfir 卡片规定，当读写器(PCD)与卡片(PICC)进行 DES/3DES 运算时，卡片总是进行加密运算，与之对应，读写器总是进行解密运算。DES 密钥有 16 个字节，如果前 8 个字节与后 8 个字节相同，则进行 DES 运算，反之如果前 8 个字节和后 8 个字节不同，则进行 3DES 运算。如下表所示：

使用密钥	PICC	PCD
KEY1：3DES 密钥的前 8 个字节	加密	解密
KEY2：3DES 密钥的后 8 个字节	解密	加密

KEY3：3DES 密钥的前 8 个字节	加密	解密

DES/3DES 运算每次操作 8 字节，如果数据不足 8 字节，必须填充为 8 字节，填充的数据通常是 00，如果正好要进行 DES 运算的数据是“00 00 00”（比如“读取所有数据”命令），则填充一个 0x80，后面再填充 00。

所有的 DES/3DES 操作使用密码块链接模式（CBC），即上一次 DES 运算的结果作为下一次运算的初始向量。发送数据使用发送 CBC 模式，接收数据使用接收 CBC 模式。第一次运算的初始向量规定为 8 字节的 00.

以下描述 3 次握手认证和段密码产生的过程及实例，假设卡片密码为 16 个 00：

第一步：读写器作为发起认证的主导方，向卡片发送认证(Authenticate)命令，并携带一个表示密码序号的参数(卡片上每种应用可以最多有 14 组不同的密码，其序号为 0-D)。如果选定的应用标识符 AID 为 0，那么认证将指向卡片的主密码(卡片密钥)，在此情况下，密码序号必须为 0。如果 AID 不为 0，则认证的是某一应用的密码。卡片进入磁场上电复位后将默认选中 AID 为 0。也就是说卡片复位的首次密码认证总是指向卡片主密码。如果卡片上不存在指定的密码组号，卡片将返回一个错误码。

第二步：卡片用读写器指定的密码加密一组 8 字节的随机数 RndB，例如 RndB = 98 E4 EE 2E 8B 4B F7 B1，加密方法使用 DES/3DES，其结果用 ek（RndB）表示，此处 ek（RndB）= 61 58 F4 51 8A 25 9B 00，并把 ek（RndB）返回给读写器。

第三步：读写器用待认证的密码 16 个 00，对收到的 ek（RndB）进行 DES/3DES 解密从而得到 RndB = 98 E4 EE 2E 8B 4B F7 B1。接下来读写器对 RndB 进行 8 位闭合左循环，从而将第一个字节移到了最后一个字节的位置，结果记为 RndB'，RndB' = E4 EE 2E 8B 4B F7 B1 98。然后读写器自己产生一个 8 字节的随机数 RndA，例如 RndA = 00 11 22 33 44 55 66 77,并与 RndB' 连接起来组成 RndA+RndB' = 00 11 22 33 44 55 66 77 E4 EE 2E 8B 4B F7 B1 98 共 16 字节，使用 CBC 模式的 DES/3DES 解密运算，得到的结果称为 dk（RndA+RndB'）= 74 F4 AE 77 7A A4 31 E8 4B 18 BA 8F 74 CF 80 63 发送给卡片。

第四步：卡片收到 16 字节 dk（RndA+RndB'）后执行 DES/3DES 加密运算，得到结果 RndA+RndB'。卡片首先将自己原来的 RndB 大循环左移 8 位，看结果是否等于 RndB'，如果不相等，卡片将停止认证过程，并回送一个错误码。如果相等，证明卡片使用的密码和读写器使用的密码一致，卡片将获得的 RndA 也大循环左移 8 位得到 RndA' =11 22 33 44 55 66 77 00，然后对 RndA' 进行 DES/3DES 加密运算，得到的结果称为 ek（RndA'）=F1 81 F7 32 6D CD 86 A6 回送给读写器。

第五步：读写器收到 ek（RndA’）后执行 DES/3DES 解密从而得到 Rnd A’，并把自己之前产生的 RndA 大循环左移 8 位，得到的结果与 Rnd A’比较，如果不相等，读写器将退出认证过程并可将卡片休眠。

第六步：卡片将当前的应用设置为通过认证状态，如果 AID=0，则将卡片本身设置为通过认证状态。

第七步：如果双方所有的比较都成功，通过组合 RndA 和 RndB 得到一个 16 字节的段密码，组合的方法如下：

段密码=RndA 第一部分+RndB 第一部分+ RndA 第二部分+RndB 第二部分

对于本文中的例子，产生的段密码为

00 11 22 33 98 E4 EE 2E 44 55 66 77 8B 4B F7 B1

之所以采取这种组合方法产生段密码是为了避免恶意的读写器通过将 RndA=RndB 而将 3DES 运算强行转化为 DES 运算。如果之后的数据传输确实想使用单 DES 操作（使段密码的前 8 字节与后 8 字节相等），应使用前 8 个字节，即 RndA 第一部分+RndB 第一部分，而不能使用后 8 个字节。

得到 16 字节的段密码后，3 次相互握手认证完成。如果之后的通讯是 DES/3DES 加密传输，则使用刚产生的 16 字节段密码作为临时的 DES 密钥。