

Mifare®DESFire

Chris Stanford
CJS Technology
Chris@cjstechnology.com



Mifare®~~DESFire~~



Its not really anything like Mifare

Which is just as well!

As the Card we all know as Mifare
is somewhat discredited

Whereas *DESFire* never did work
in the same way!

A marketeers dream gone wrong?

DESFire

Is specified by ITSO

*DESFire is ITSO Customer Media
Definition seven (CMD7 for short)*

*The ITSO specification is based on
revision 3.1 of Mifare® DESFire*

*This means that all fully certified
POSTs will read and write onto this
version*

DESFire CMD7 *Vs latest DESFire version*

It uses the published and credible Triple DES security algorithm which has, not yet, been broken.

In short- it is far better than Mifare® Classic

And in more recent versions it has gained:

- 2K,4K and 8K memory size options
- Improved relay attack prevention
- AES with longer keys

Can the new version be used within ITSO?

DESFire CMD7 Vs latest DESFire version

2K,4K and 8K memory sizes

The new version with 4K or 8K memory can be configured by Personalisation bureaux to comply exactly with CMD7

The 2K version likewise. But, using ITSO default settings will limit the size of any other applications

In either case no material changes to the ITSO specification are needed and publishing an ITSO Design guide to ease use of the new version should suffice

DESFire CMD7 Vs latest DESFire version

Improved relay attack resistance

The CMD7 version of DESFire does protect the content of all messages from this form of attack however there is a minor weakness that the new version of DESFire addresses

To address this minor weakness both POST and ISAM applications would need to be changed

DESFire CMD7 Vs latest DESFire version

AES with longer keys

Some background about DES and AES is required

DESFire CMD7 *Vs latest DESFire version*

DES

DES was standardised in 1977

It has remained since then credibly secure in its triple DES form

Triple DES as used by ITSO is also used by the payment industry (EMV) and is estimated to remain in use for about 10-15 more years.

DESFire CMD7 *Vs latest DESFire version*

AES

AES is a youngster when compared to DES
having only been standardised in 2002

But in 2005 the NIST (USA) showed growing
confidence in AES by substituting it for the
the DES standard

DESFire CMD7 Vs latest DESFire version

Can the new version be used within ITSO?

YES! The enhanced memory options can already be supported by the existing POST and ISAM applications

Blocking the minor relay attack weakness would require Changing the POST and ISAM application.

YES! As this feature does not prevent the new version of DESFire from being used modifying applications is not really necessary at present.

DESFire CMD7 Vs latest DESFire version

Can the new version be used within ITSO?

YES! BY the continued widespread use of Triple DES for some years to come

However ITSO remains vigilant of the movement to AES from DES.

ITSO is already considering the technical requirements for adding the AES algorithm to a new version of the ISAM which could replace existing ISAMs as they become life expired.

After this time the use of AES based CM security on any platform becomes viable

DESFire Compared to other CMDs

ITSO CMD	Common Name	Mutual authentication	Replay prevent	Relay attack prevent	Speed	Cost
8	Calypso	Strong	Strong	Strong	Fast	Medium
2	JCOP	Strong	Strong	Strong	Slow to Medium	Higher
7	DESFire	Strong	Strong	Less Strong	Fast	Lower
1,3	Mifare Classic	Too Weak	Too Weak	Too Weak	Fast	Lowest

Notes:

Transaction speed is mainly influenced by the design and function of the HOST system, this comparison gives a relative indication only and faster JCOP implementations are on the way

Cost is very dependant on total volumes produced as well as quantities ordered

Mifare®DESFire

The choice of CM by ITSO licensed Members should take into account

- Capability
- flexibility
- Security
- Availability
- Price

All of these things are important when considering the business needs and acceptable risk

DESFire is a much more trustworthy successor to Mifare®Classic but, where cost justified, other CMDs may be more suitable for broader business needs.

Thank You!

Chris Stanford
CJS Technology
Chris@cjstechnology.com

