

A banner image featuring the word "RFID" in large, white, 3D-style letters on the left. To the right, a pair of hands is shown holding up a glowing green starburst shape against a background of a blue sky with white clouds. The starburst has several green lines radiating from its center.

RFID

Mifare RFID Tags : A Short Buyer's Guide

Improved Security, Backward Compatibility

Mifare RFID tags are one of the most widely used tags for applications needing some security component. However, in the last few years, the original version of Mifare has been shown to have limitations that allowed its security to be compromised. Earlier Mifare Classic tags also have reached their limit of unique ID's.

NXP, the developers, have responded with two new versions of Mifare tags; the Mifare Plus S and Mifare Plus X.

Comparing the Mifare Tag Families

Mifare tags were the basis of the original "contactless smart card" and have been widely used for payment card and ticketing applications. NXP Semiconductors, the patent holders for the Mifare chip, estimate that over 1 billion chips and over 10 million readers have been sold worldwide since the Mifare family was first introduced in 1992.

The Mifare tag has been used in such applications as 2006 Football World Cup tickets, Moscow metro, London's Oyster Card, and at Imperial College London and other institutions for student and staff identity and access cards.

The Mifare tag's security algorithm is used to authenticate the tag to a reader and to protect the confidentiality of the data stored on the card. When the Mifare Classic was first introduced in 1994, a proprietary algorithm (Crypto-1) was developed to provide a robust level of security and acceptable performance. However, since that time chip storage and performance have improved making the use of standardized algorithms practical. Also the abilities of the criminal community have improved and the computing power available for security attacks has increased greatly.

In 2007 the first weaknesses were made public and in 2008 a research group demonstrated that it was possible to clone and manipulate the contents of a Mifare Classic card.

To address these issues NXP developed a new range of Mifare chips; the Mifare Plus.

These chips offer new users a secure system and users of existing Mifare Classic based tags the important facility of combining compatibility with existing systems with the potential for subsequent upgrade to a more secure platform.

Of course, simply implementing the Mifare Plus card on an existing Mifare Classic based application does not bring any security benefit. However, the Mifare Plus solution allows the security level on a tag to be stepped up once the tag is in use. So, new Mifare Plus tags can be issued (with compatibility with an existing solution) and at a future point upgraded when the rest of the solution is upgraded.

New users of Mifare, can of course, get the benefits of the improved security provided by Mifare Plus straightaway. The standard version (Mifare Plus S) provides access to AES (Advanced Encryption System) with its 128 bit encryption key but the greatest improvement is offered by implementing Mifare Plus X. A range of additional facilities become possible because of the extended ("eXpert") command set but the most important feature of the Mifare Plus X tag is its ability to provide a mixed mode security solution combining the performance capabilities of Crypto-1 and the robust security facilities of the AES standard. Plus X cards also support proximity checking, a technique designed to prevent cloning attacks by relaying data with unauthorized accesses.

The differences between the main types of Mifare tags are:

Tag Type	Mifare Classic	Mifare Ultralight	Mifare Ultralight C	Mifare DESfire & DESfire X	Mifare Plus S	Mifare Plus X
Introduced	1994	2008	2008	2002	2009	2009
Application	Reusable Fare Cards	Disposable Tickets / No Security	Low cost applications using DES encryption	Re-usable cards with DES encryption	Successor to Mifare Classic with improved security	As Mifare Plus but with more facilities
On-chip Data Storage	1k, 4k or 320 bytes	512 bits	1536 bits	2k, 4k 8k bytes	2k or 4k bytes	2k or 4k bytes
Encryption Standard	Proprietary	None	ISO1443 A1-3	ISO1443 A1-3	Proprietary or ISO1443 A1-3	Proprietary or ISO1443 A1-3
Encryption Algorithm	Crypto-1	None	DES	DES	Crypto-1 Or AES	Crypto-1 Or AES
Encryption Key Length	48 bit	None	128 bits	128 bits	48 bits or 128 bits	48 bits or 128 bits
AES Security					CMAC	CMAC/ Encipher
Unique Chip ID	4 bytes	7 bytes	7 bytes	7 bytes	7 or 4 bytes	7 or 4 bytes
Additional features					Mifare Plus S tags can be used in a system which initially gives compatibility with Classic cards but then is upgraded to full AES security.	As Mifare Plus S but also supports the combined use of AES for authentication (high security) & Crypto-1 for date confidentiality (high performance). Proximity check against relay attacks.
Typical Price (100x ISO card)	\$84 - \$110	\$64	\$70	\$150-205	(No Pricing Available)	\$93 - \$121

CoreRFID's Capabilities

CoreRFID is happy to provide Mifare Plus S or Mifare Plus X tags and to work with users on the implementation of projects using these technologies. CoreRFID can also provide a full range of personalisation services for Mifare tag based cards including such facilities as card overprinting, embossing, photo engraving and so on.

Please also see our fact sheet: 077 Mifare Codes FAQ for guidance on issues surrounding the 4 byte unique identifier limit.

About CoreRFID

Contact us today:

CoreRFID Ltd, Dallam Court, Dallam Lane, Warrington, U.K. WA2 7LT

T: +44 (0) 845 071 0985 F: +44 (0) 845 071 0989 W: www.corerfid.com E: info@corerfid.com