

CARD TECHNOLOGIES

for

RFID card readers and door controllers

October 2022

100-02837-M2022-04-01-CARD TECHNOLOGIES



Third Millennium Systems Limited



Introduction

The following pages offer a brief outline to some of the most common RFID card technologies available, together with their respective security levels and capabilities.

The list is by no means exhaustive, but gives a comparison of technical information against which an installer, or end-user, might make an informed decision.

About Us

Third Millennium has become a multi award-winning manufacturer of advanced access control readers, and specialises in the introduction of new technologies to the access control market.

Supplying many of the world's leading security specialists, our products offer innovative style, coupled with the broadest range of RFID technologies available ...

... all from a SINGLE manufacturer.



Third Millennium Systems Limited

SECURITY LEVEL

Comparison of RFID card technologies used by Third Millennium Systems Ltd.

SECURITY LEVEL	125 kHz	MIFARE® CSN	MIFARE® Classic	MIFARE® Classic SE	MIFARE® DESFire® SE	LEGIC
Summary	Very Low Security	Low Security	Mid Security	High Security	Best Practice	Best Practice
Encryption	NONE	NONE	CRYPTO1 48-bit	CRYPTO1 48-bit	AES 128-bit	AES 128-bit
Secure Envelope	NONE	NONE	NONE	3 x AES 128-bit Keys	3 x AES 128-bit Keys	3 x AES 128-bit Keys
Additional Security Features	NONE	NONE	NONE	Diversified Keys with AES-128 bit generated MAC	Diversified Keys with AES-128 bit generated MAC	Diversified Keys with AES-128 bit generated MAC
Can Be Duplicated	YES	YES	YES	NO	NO	NO

'MIFARE', 'MIFARE Classic' and 'MIFARE DESFire' are trademarks of NXP B.V.

'LEGIC' is a trademark of LEGIC Identsystems



Third Millennium Systems Limited



125 kHz

- Wide range of formats.
 - Prox
 - GE Casi
 - Farpointe
 - Kantech
 - etc.
- Read by a wide variety of manufacturers.
- Cheap cost of credential.
- Easy to duplicate.





MIFARE® CSN

- Cards ready 'to go' from the factory. No encoding required.
- Read by a wide variety of manufacturers.
- Limited number scope, unable to specify a range.
 - Could result in clashes with a large user base.
- Easy to duplicate.



MIFARE® Classic

- Choice of format – can be customer specific.
- Reader needs specific configuration.
- Additional data can be written, if there is space.
- Can be duplicated.
 - But takes some effort.

Third Millennium Secure Envelope

- Builds security features on top of the card.
 - Can no longer be duplicated.



MIFARE® DESFire®



Registered Partner

- Choice of format – can be customer specific.
- Reader needs specific configuration.
- Additional applications may be written.
 - Verified application IDs managed by NXP.
 - More options than MIFARE® Classic.
- No known methods to duplicate.

Third Millennium Secure Envelope

- An additional layer of security to ensure future resilience.



Third Millennium Systems Limited

LEGIC

PARTNER

prime / advant

LEGIC

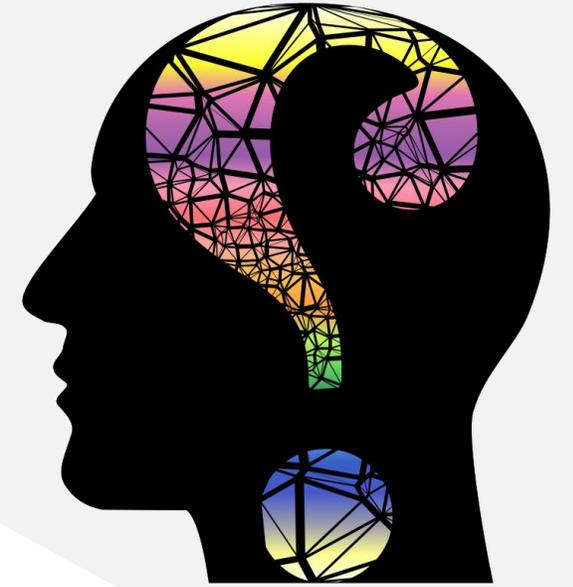
- Reader requires specific configuration.
- No known methods to duplicate.
- Keys and technology managed by LEGIC.
 - Often, an end user will have ownership of their own keyset obtained directly from LEGIC.



Third Millennium Systems Limited

Card Formats

- Within reason, if a card is encoded, that encoded data could be anything.
- Some common formats include:
 - Sensor 26-bit (H10301)
 - Geoffrey 34-bit
- More bits give more space for more data.
 - You can have increased card number ranges and more possible facility codes.
- The card format must be entered on the controller, so it can recognize how to use and check the data it receives.
 - If you use a common format, it may already be entered for you.



Secure Envelope DEEP DIVE



- Third Millennium's Secure Envelope (SE) is a smartcard encoding method that enhances the credentials' functionality, and data security.
- Secure Envelope mitigates duplication threats to MIFARE® Classic, by:
 - AES 128-bit encryption of the access control data with 3 keys.
 - Diversified keys with AES 128-bit generated MAC (each card has a unique set of keys).
- Reader output format is stored on a card in the Secure Envelope.
- Custom SE keyset can be encoded on MIFARE® Classic or MIFARE® DESFire® platforms.
- Available SE keysets:
 - Third Millennium (standard on RX*80 and RX*90 product lines).
 - Customer specific.
 - End-user specific.



Credentials

- ISO Cards, Fobs and RFID patches (stickers).
- Optimized for best performance and read-range on **RX^{SERIES}** readers.
- High quality cards enable complete overprinting.
- Various multi-technology options.
- Added value services:
 - Custom encoding.
 - Standard and custom print.
 - Anti-duplication security features can be incorporated:



Registered Partner



prime / advant

- Holo-Design
- Holo-Image
- Invisible UV
- MicroText
- Guilloche pattern / Watermarks
- Graphics, format and layout design
- Card bureau service



Third Millennium Systems Limited

'MIFARE', 'MIFARE Classic' and 'MIFARE DESFire' are trademarks of NXP B.V.

'LEGIC' is a trademark of LEGIC Identsystems

Contact Us

Third Millennium Systems Ltd
18/19 Torfaen Business Centre
Panteg Way, New Inn
PONTYPOOL
NP4 0LS United Kingdom



+44 (0) 1495 751 992



www.tm-readers.com



info@tm-readers.com

