MIcommunity Q & A

Where do I find MIFARE datasheets?
Many data sheets for MIFARE products, i.e. MIFARE Classic or MIFARE Ultralight, are available for download on www.nxp.com. Some require registration on NXP docstore (www.docstore.nxp.com) after that the documents can be downloaded or ordered. Nevertheless, secure products like MIFARE Plus or MIFARE DESFire EV1 require an NDA to be in place. Your local NXP sales representative supports you in setting up such an NDA.

What is the difference between MIFARE DESFire EV1 v04 and v05?
Both versions use the same silicon. The only difference is a small change in the startup sequence to make V05 more robust in noisy/non-ISO environments.

Is MIFARE Plus or MIFARE DESFire more secure?
Both devices have the same level of security, and they differentiate essentially through their memory structure and functionality

How can I emulate a MIFARE card on my NFC enabled mobile phone?
Currently there are three main possibilities to get MIFARE capabilities onto your phone
Your phone is equipped with an embedded secure element (eSE) with MIFARE capabilities by the OEM (original equipment manufacturer) (eSE available from NXP and its licensees)
Your mobile network operator is using a SWP SIM (single wire protocol) with MIFARE capabilities (available from NXP's licensees)
You are using a microSD card with MIFARE capabilities and the NFC controller in the phone or a microSD with its own RF-interface.

What is MIFARE4mobile?
MIFARE4Mobile is an interface specification to enhance the of MIFARE capabilities on a secure element (eSE, SWP SIM, µSD) with harmonized interfaces for over the air (OTA) provisioning and lifecycle management of MIFARE applications and wallet interaction. More information can be found on www.mifare4mobile.org

What is the advantage of using MIFARE Plus in Security Level 2?
Security Level 2 is a possible migration path from MIFARE Classic based systems where MIFARE Classic CRYPTO1 keys are randomly derived from a mandatory AES authentication. The transport layer (ISO/IEC14443-3), commands and protocol are similar like MIFARE Classic.

How can I be sure that if I buy MIFARE Classic 4B NBUID ICs I will not have repeated UIDs with my system cards.
NXP provides the list of NUIDs which each shipment (wafer or reel). The value chain (i.e. inlay manufacturer, card manufacturer) can pass this information onto the end customer in advance to know which NUIDs they will receive.

What is the difference between the CRC used for the MIFARE communication and the CRS (or block check) of the UID and how do I use it?
The 2-byte CRC is added by the reader / card automatically to the transferred bytes to ensure communication integrity; the check-byte is added to the 4byte SNR (also referred to as UID) to verify the correct transmission of the UID.

What is the resonance frequency of MIFARE cards?
There is no certain value specified for the resonance frequency of MIFARE cards in the ISO/IEC 14443. This ISO standard specifies the measurement of the card's parameters, like load modulation, at the frequencies of 13.56 MHz and 19MHz. The independent test MIFARE Certification Institute AIT specifies a resonance frequency of 14.5 ... 18.5 MHz for MIFARE cards.
The new "Card Coil Design Guide" recommends 13.56 ... 170 MHz depending on the card antenna classes.

Why is it impossible to authenticate using Key B for the first card access in MIFARE Classic?
During production the standard delivery access conditions are set in a way that key B is readable. The access conditions for MIFARE Classic and MIFARE Plus do not allow using a key for memory access commands (although the authentication is successful with this key) when this key is readable. E.g., it is not possible to read or write data in a sector, when this sector has been authenticated with key B and when this key is readable.

Is it possible to use only one key for MIFARE Classic?
It is possible to use only one key, that means only key A can be used. The 6 bytes allocated for key B can be used as additional memory. We recommend not to use this additional memory, because every time data is written to that sector trailer, key A and the access conditions itself have to be written too.

How many read/write operations can be executed on a MIFARE card and is there a difference between MIFARE Classic and MIFARE Ultraligh?
You can find a value for the number of write cycles + data retention time for EEPROM access in the data sheet. Reading an EEPROM doesn't have an impact on the endurance of the EEPROM, so there is no limit for the number of reads.
Examples:
MIFARE Classic next generation 1K, 4K: 200k read/write cycles + 10 years data retention
MIFARE Ultralight 10k read/write cycles + 5 years data retention.

When presenting 2 MIFARE cards (stacked on top of each other) into the Micore Reader field, the operating distance increases dramatically. What does this indicate about the antenna tuning?
The increase of the distance with two cards is quite normal. MIFARE cards are tuned to a resonance frequency of 14 ... 17.5 MHz. Two cards close together detune themselves down towards the 13.56 MHz. This increases the induced voltage that powers the MIFARE chip. On the other hand the current (I TVDD) should be watched to make sure, that the reader antenna is not detuned too much, when changing the environment (whatever this may be: a hand, a metal plate, two or more cards, etc. coming close to the reader antenna). This current is a good indicator of changes in the magnetic field (=power) distribution. A slight change of the current (<10 - 20%) is OK, but with a bad antenna matching the current may change more than 50% (or even up to or more than 100%!).

The MIFARE DESFire and MIFARE Ultralight use a cascade tag of “0x88”. What does that mean?
According to the ISO14443A-3 the value of "0x88" shall not be used as UID0 in single size UIDs (first byte). In double size UIDs this first byte in the cascade level 1 answer is called "cascade tag" (CT) and contains "0x88". In triple size UIDs this first byte of the cascade level 2 and 2 answer is called CT and contains "0x88". The CT always forces a collision with single size UIDs to ensure a proper selection.
Remark:
The UID3 of double UIDs shall not contain "0x88" to always force a collision with triple size UIDs. This is not specified in the ISO14443A-3, but is guaranteed for NXP ICs. Competitor ICs according to the ISO14443A-3 always force a collision with NXP ICs even if they use "0x88" in their UID3 of a double size UID: double and triple size UIDs always contains the manufacturer code in UID0, which is unique for NXP ICs (0x04).

I want to use my reader with NXP chip (eg RC531, RC 523) to support MIFARE DESFire (or Plus). Does NXP provide the library?
Yes, NXP provide reader libraries for all our reader chips supporting every MIFARE products. However, libraries for security products like MIFARE DESFire and MIFARE Plus can only be obtained a valid NDA. Some countries/regions are export controlled, therefore the reader library can only be provided without security algorithm.

Can I have MIFARE Plus in an export controlled country?
Yes, “MIFARE Plus S” is not Export Controlled.

I want to use MIFARE cards with MIFARE SAM, is there any guidance to implement?
We have implementation hints documents for each MIFARE product explaining the usage with MIFARE SAM card.

My system design requires a dynamic memory structure in card, which product could I use?
MIFARE DESFire offers a flexible file system where applications and files can be tailored to any application needs.

I want to secure my card authentication with AES crypto algorithm, which product could I use?
Both MIFARE Plus and MIFARE DESFire EV1 offer AES authentication.

Can I configure my card to read only after its personalization?
For MIFARE Classic and MIFARE Plus you can use access condition settings. By not granting Key A and Key B for write, it will behave like read-only. For MIFARE DESFire chose “never” while configuring the file’s write access.

We have a MIFARE SAM AV2 sample card which seems to not support AV2 commands?
All MIFARE SAM AV2 cards delivered in AV1 mode, you need to switch first to AV2 mode to use AV2 commands.

In my system different kinds of MIFARE products are used. Before running card specific commands how can I know the card type?
You can use the SAK code that you will receive after the card activation. Every MIFARE Product gives different SAK codes.
Special care has to be taken in case you are wanting to allow for products i.e. NFC enabled mobile phones or multi application Smart Card Controllers that could support multiple MIFARE technology platforms (such as MIFARE Classic, MIFARE Plus, MIFARE DESFire) in future. In such a case you should expect a “neutral” SAK as any other value would limit the concurrent co-existence of different products at activation time. Please refer to the respective application notes provided by NXP.

Can I assign my own UID to MIFARE cards?
UIDs for MIFARE cards are assigned during the production and it can never be changed thereafter.