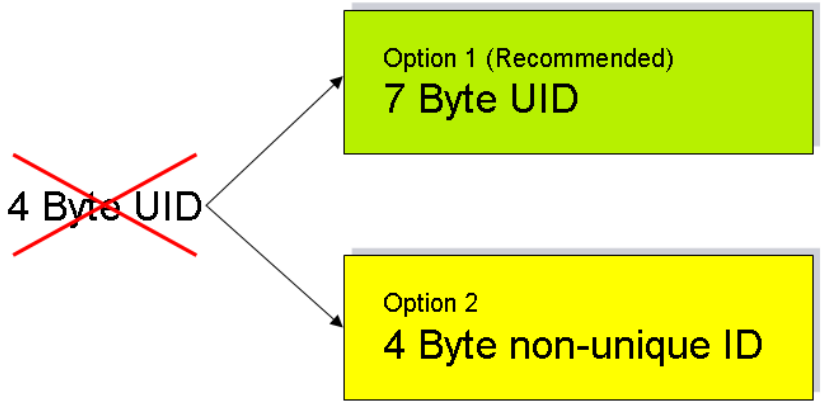
4 Byte and 7 Byte UID offering for MIFARE Classic™, MIFARE Plus™, SmartMX™ and licensed products

Questions and Answers

Background

In Q2 2010 NXP customers have been informed of important updates on the IDs of MIFARE Classic and related products.



Unique 4 Byte IDs will be discontinued. Customers will have the choice to purchase either products with unique 7 Byte IDs (our recommended option) or 4 Byte IDs, which are not globally unique any more.
This document lists common questions and our answers on the topic.

Content

General Questions 4
What is a unique identifier number and what is it used for? 4
What is the difference between a 4 byte UID and a 4 byte ID? 4
General Questions 5
MIFARE Classic is a fundamentally flawed product, which has been hacked by several research groups. Why does NXP even extend its lifecycle by providing 7 Byte UID solutions for it? 5
Would this situation not be a big opportunity to discontinue MIFARE Classic and provide more secure solutions to the market? 5
Visibility on end of life of 4 Byte UID based products 6
Is only MIFARE Classic 1K concerned? 6
Quantity of unique numbers left over? 6
Communication plan of NXP towards the market regarding the need to change to 7 Bytes UID 7
Towards system integrators (SIs) 7
Towards public transport operators (PTOs)? 7
What will be the timing of the planned communication? 7
Communication plan of NXP towards the market regarding the need to change to 7 Bytes UID 8
What will NXP do to educate the market? 8
Focused on MIFARE Classic only? 8
Focused on MIFARE Classic 1K only? 8
Impact on MIFARE Plus 9
Impact on 4 B UID version of MIFARE Plus? 9
Will all 8 possible versions remain available? 9
Is any simplification of MIFARE Plus range now foreseen? 9
Impact on MIFARE Plus 10
Given the UID choices for MIFARE Plus will most operators not just choose 4 Byte UIDs by default? 10
Scheduled availability for MIFARE Classic 7 B UID 11
MIFARE Classic 1K with 7 B UID 11
MIFARE Classic 4K with 7 B UID 11
Impact on MIFARE Implementations NXP SmartMX ICs 12
Is the SmartMX dual-interface controller only available with 4B UID? 12
Will the next generation of dual interface chips have a 7 B UID for MIFARE Classic emulation? 12
Impact on Fast Pay ICs 13
Is NXP's Fast Pay product affected by the 4B UID issue? 13
Impact for products from 3rd parties 14
On pure contactless transport chip from Infineon Technologies 14
On implementations of NXP licensees? 14
Implications for other NXP smart card ICs 15
Are MIFARE Ultralight, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1 and MIFARE Plus (7 B UID version) ICs also affected by the 4 B UID issue? 15

Impact on reader infrastructure 16
Is the existing reader infrastructure able to support 7 B UID? 16
Impact on reader infrastructure 17
Until when does NXP think that the existing reader infrastructure will be able to support 7 B UID? 17
Impact on reader infrastructure 18
Which solutions does NXP offer in case systems do not support 7 B UID? 18
Impact of “non-unique IDs" to existing systems 19
What do non-unique IDs mean for the legacy infrastructure? 19
Is this really usable as we state that uniqueness is key? 19
Differences of 4 B UID vs. 7 B UID 20
Are there any differences between a 4 B UID MIFARE Classic and a 7 B UID MIFARE Classic beyond the card activation ("Anticollision")? 20
Impact of the 4 / 7 B ID topic on NFC 21
Do all NXP NFC IC's (PN51x, PN53, PN54x and PN65x) support a 7 Byte MIFARE UID ? 21

General Questions

What is a unique identifier number and what is it used for?

ISO/IEC 14443 Type A defines a Unique IDentifer to be used for card selection and activation. The standard defines single, double and triple size UIDs which correspondingly consist of 4, 7 and 10 Byte. In many contactless systems, the UID is not only used for card activation but also as a logical reference i.e. in a background system to the card itself

What is the difference between a 4 Byte UID and a 4 Byte ID?

A 4 byte UID is an identifier which has been assigned by the card manufacturer using a controlled database. This database ensures that a single identifier is not used twice. In contradiction, a 4 byte ID is an identifier which may be assigned to more then one contactless chip over the production time of a product so that more then one card with the same identified may be deployed into one particular contactless system.

General Questions

MIFARE Classic is a fundamentally flawed product, which has been hacked by several research groups. Why does NXP even extend its lifecycle by providing 7 Byte UID solutions for it?

The security of systems does not rely on the security of a smart card IC alone. Many MIFARE Classic based systems have been secured by countermeasures until a migration to stronger security is possible.

Would this situation not be a big opportunity to discontinue MIFARE Classic and provide more secure solutions to the market?

For applications that require a higher level of security, we recommend to migrate from MIFARE Classic to MIFARE Plus or MIFARE DESFire EV1 with 7B UIDs.

Visibility on end of life of 4 Byte UID based products

Is only MIFARE Classic 1K concerned?

No, the 4 B UID issue affects all ISO/IEC 14443 Type A products including MIFARE Classic products (MIFARE Classic 1k and MIFARE Classic 4k), MIFARE Plus as well as all MIFARE Classic implementations on NXP‘s SmartMX and JCOP products the 4 B UID issue also affects Infineon Technologies and NXP’s MIFARE licensees

Quantity of unique numbers left over?

The exact quantity could only be estimated as NXP is not aware of quantity of unique numbers left over at Infineon; in any case, we expect the market will run out of 4 Byte unique IDs end of **2010** this will affect NXP and MIFARE licensees as well as Infineon

Communication plan of NXP towards the market regarding the need to change to 7 Bytes UID

Towards system integrators (SIs)

Yes, NXP will be in close contact with leading SIs from week 12 onwards.
The message is that the market will run out of 4 Byte unique IDs by the end of 2010**.**
Our default successor product is based on 7 Byte unique IDs.
Our recommendation is to move to 7 Byte unique IDs.

Towards public transport operators (PTOs)?

Yes, NXP will be in close contact with selected PTOs in alignment with the respective SIs from week 12 onwards.
Same message and recommendation as for system integrators.

What will be the timing of the planned communication?

We are distributing a customer letter to the wider MIFARE eco-system in May 2010
In addition, we plan to run several roadshows, trainings and webinars in 2010

Communication plan of NXP towards the market regarding the need to change to 7 Bytes UID

What will NXP do to educate the market?

We have planned a very active communication including several roadshows, trainings and webinars in 2010. We will engage with leading SIs, PTOs, reader manufacturers, card makers, banks and handset makers.

Focused on MIFARE Classic only?

4 B UID issue affects all MIFARE Classic products. Therefore, the communication will be focused on the whole MIFARE Classic portfolio.

Focused on MIFARE Classic 1K only?

No, communication will be focused on whole MIFARE Classic portfolio.

Impact on MIFARE Plus

Impact on 4 B UID version of MIFARE Plus?

As MIFARE Plus also covers a 4 B UID option during the migration period, we will inform our customers regarding the end of life of MIFARE Plus with 4 B UID.

Will all 8 possible versions remain available?

Yes, all current MIFARE Plus versions remain available; however we focus on specific high runners and we will inform the market about the end of life of MIFARE Plus with 4 B UID

Is any simplification of MIFARE Plus range now foreseen?

We focus on specific high runners; these are

- MIFARE Plus S 2K 7 B UID
- MIFARE Plus X 4K 7 B UID
- MIFARE Plus S 2K 4 B UID (only during short migration period, then 4B ID or 7 B UID)
- MIFARE Plus X 2K 4 B UID (only during short migration period, then 4B ID or 7 B UID)

For those products we keep buffer stocks for immediate supply; others will be delivered with longer lead times.

Impact on MIFARE Plus

Given the UID choices for MIFARE Plus will most operators not just choose 4 Byte UIDs by default?

NXP is clearly recommending MIFARE Plus with 7 B UID;

MIFARE Plus ICs with 4 BUID are being offered only during the relatively short migration period, where backwards compatibility is necessary.

A migration to higher security level on the system side should always be used to enable the acceptance of 7 B UIDs.

After the migration our default product offering is 7 B UIDs. We inform the market about the end of life of MIFARE Plus with 4 B UID, which is also expected around end of 2010.

Scheduled availability for MIFARE Classic 7 B UID

MIFARE Classic 1K with 7 B UID

First samples are already available. Commercial product will be released in May 2010. In addition, we will launch an improved version with respect to read range and personalization options in H1 2011
→ these personalization options will allow our customers to optimize their stock handling and to reduce the probability of problems with existing reader infrastructures.

MIFARE Classic 4K with 7 B UID

Same schedule as for MIFARE Classic 1K 7 B UID

Impact on MIFARE Implementations NXP SmartMX ICs

Is the SmartMX dual-interface controller only available with 4B UID?

No. The SmartMX family has been and will remain to be available with 7B UID when not ordering a MIFARE Classic emulation.

Will the actual SmartMX controller family been developed towards 7B UID for MIFARE CLASSIC ?

Yes, the actual SmartMX controller family based on CMOS14 will be extended to also support the 7Byte UID for MIFARE Classic. The exact timeline will be announced later this year.

Will the next generation of dual interface chips have a 7 B UID for MIFARE Classic emulation?

Yes, the next generation of dual interface is called P60 and the chips will have a 7 B UID option for MIFARE Classic emulation. The exact timeline will be announced later this year.

Impact on Fast Pay ICs

Is NXP's Fast Pay product affected by the 4B UID issue?

No, Fast Pay uses 7B UID and is therefore not affected.

Impact for products from 3rd parties

On pure contactless transport chip from Infineon Technologies

NXP has aligned the use of 4 B UID ranges with Infineon Technologies.

On implementations of NXP licensees?

NXP has aligned the use of 4 B UID ranges with its MIFARE licensees.

Implications for other NXP smart card ICs

Are MIFARE Ultralight, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1 and MIFARE Plus (7 B UID version) ICs also affected by the 4 B UID issue?

No, the above mentioned contactless ICs from NXP have 7 B UIDs and are not affected by the depletion of the 4 B UIDs.

Impact on reader infrastructure

Is the existing reader infrastructure able to support 7 B UID?

NXP does not have 100% visibility regarding all installed readers worldwide; nevertheless all NXP reader ICs can handle 4 B, 7B and also 10 B UIDs. The majority of all installations are still based on MIFARE Classic which was supporting 4 B UIDs only until today. Therefore, we assume that most existing infrastructure does not support 7 B UID for MIFARE Classic yet; we assume that from this year onwards, existing infrastructure will migrate to 7 B UID support for MIFARE Classic.

Please keep in mind that all other installations using smart card ICs from NXP such as MIFARE Ultralight, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1 and MIFARE Plus (7 B UID version) are already able to cope with 7 B UIDs.

Impact on reader infrastructure

Until when does NXP think that the existing reader infrastructure will be able to support 7 B UID?

NXP does not have 100% visibility regarding all installed readers worldwide. Nevertheless all NXP reader ICs can handle 4 B, 7B and also 10 B UIDs. We assume that from this year onwards, existing reader infrastructure will migrate to 7 B UID support for MIFARE Classic. We assume that this process will take at least until 2015 and may go beyond.

NXP actively contributes to the ISO/IEC 14443 standard which was published in 2001 and strongly recommends and supports to build readers according to that standard.

Every fully ISO/IEC 14443 compliant reader can handle 4 B UIDs, 7 B UIDs and 10 B UIDs.

Impact on reader infrastructure

Which solutions does NXP offer in case systems do not support 7 B UID?

For systems that are not able to support 7 B UIDs, NXP offers the following options to ensure sustainable operation of those MIFARE Classic installations:

We will continue to supply MIFARE Classic ICs with 4 Byte identifiers; these 4 B IDs will be based on selected ID ranges out of the old NXP 4 Byte range

We will give recommendations on how to do the best map of a 7 Byte UID into a 4 Byte ID range.

In addition, NXP will offer a downloadable list of the IC identifiers which are used for each reel or wafer. This enables pro-active impact analysis before issuing new cards into contactless systems.

In any case, as uniqueness is often considered to be an important part of a contactless e-ticketing system (e.g.: wrt fare calculation, black listing, etc.). NXP strongly recommends migrating to 7 B UID.

Impact of “non-unique IDs" to existing systems

What do non-unique IDs mean for the legacy infrastructure?

For the infrastructure, there is no impact as the non-unique ID is still 4 Byte With respect to the full system, there might be the risk that cards using non-unique IDs introduce duplicates in the back-end system and therefore cause problems regarding black listing, fare calculation and card lifecycle management. Precautions have to be taken when introducing 4 B IDs into current installations based on 4 B UIDs.

Is this really usable as we state that uniqueness is key?

Yes, uniqueness is an important part of a contactless e-ticketing system (e.g.: wrt fare calculation, black listing, etc.); therefore, NXP strongly recommends to go for 7 B UID; however, the legacy infrastructure will not have completely migrated to 7 B UIDs before the market runs out of unique 4 B UIDs.
Therefore, some customers need to use 4B non-unique IDs during this migration period with the according workarounds.

Differences of 4 B UID vs. 7 B UID

Are there any differences between a 4 B UID MIFARE Classic and a 7 B UID MIFARE Classic beyond the card activation ("Anticollision")?

Yes, there can be differences on system side e.g. in backoffice databases. NXP will publish an Application Note, called "MIFARE and handling of UIDs“ where several of these differences are being addressed.

Impact of the 4 / 7 B ID topic on NFC

Do all NXP NFC IC's (PN51x, PN53, PN54x and PN65x) support a 7 Byte MIFARE UID ?

Yes, all NXP NFC hardware products can handle the 7 Byte UID. It should be noted however that the PN51x/PN53x SW Drivers only support the 4 Byte UID and the reader application software has to take about the 7 Byte UID. Dedicated application notes and updates of the user manuals will be provided to customers.