AN10969

System level security measures for MIFARE installations

Rev. 2.1 — 22 April 2020
196521

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	MIFARE DESFire, MIFARE Plus, Key diversification, Countermeasures, Attacks, Key renewal, Blacklists, Whitelists, Automatic Fare Collection, Access Control
Abstract	This Application note gives security recommendations on design contactless card systems such that they are better resilient against attacks and that the impact of attacks, if they were to succeed.

Revision history

Rev	Date	Description
2.1	20200422	Inclusion of a potential attack of withholding the CommitTransaction command in 5.5.
2.0	20170208	General update and adding new products
1.0	20100810	Initial version.

Contact information

For more information, please visit: http://www.nxp.com

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

1. Introduction

When designing contactless systems, e.g. based on MIFARE DESFire or MIFARE Plus it is important to design the system such that it is resilient against attacks, of course in a balance between costs, risks and impact when some of those risks materialize.

MIFARE DESFire EV2 and MIFARE Plus EV1 both have Common Criteria (CC) EAL5+ certification and are thereby the chips which currently have the highest certified resilience against attacks of chips for similar purposes in the industry. It means that these chips have been tested to withstand attacks with power analysis, light attacks and many more and found to be able to withstand those attacks.

Like for any chip that has Common Criteria certification of any level, MIFARE Plus and MIFARE DESFire having CC certification does not mean with absolute certainty that these chips can never be successfully attacked at any time in future. Attack methods get increasingly more sophisticated and so do the defenses that NXP builds into the chips. Unlike security in PCs, which can be generally updated and thereby increased over time, the MIFARE Plus and MIFARE DESFire chips are as they are and new defenses can (and will) only be built into future generations of chips.

The systems in which those chips are deployed can be designed such that if there ever would be an attacker being able to successfully attack the chip that the impact of this attack is limited and that the damage can be repaired.

This document describes design considerations for systems deploying MIFARE Plus or MIFARE DESFire to reduce the chances of attacks being successful and then to reduce the impact in the unlikely case that an attack was successful.

This document does not describe security design for the backend of such systems, e.g. the way in which terminals are connected to the central IT system.

This document was written with the scope of the chips that have the highest resistance against attacks. However, for other chips, like MIFARE DESFire EV1 (the predecessor of MIFARE DESFire EV2) and MIFARE Ultralight the same considerations hold. For MIFARE Classic there is a separate document, see [1], with some other countermeasures which are specific for that type of chip.

In this document, the term „MIFARE card“ refers to a contactless card with an embedded MIFARE IC.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

2. Example of a vulnerable system and a system with limited recovery opportunities

Before discussing solutions to “close the holes”, let’s look at two examples of what can be the impact of an attack on systems which are not designed to mitigate attacks or to deal with them when they occur.

2.1 Using the same key in all cards

Imagine an Automatic Fare Collection (AFC) system in a city. Let’s assume that all keys in all cards are the same. Even if there are multiple keys on a card (keyset), but the same keyset is on all cards then that makes no difference for this example.

Imagine now a criminal organization who invested a considerable amount of time and money to reverse engineer the chip in order to get a key out of a chip on a valid card for that AFC system and imagine the currently unlikely case that they succeed.

Having the key allows them to read out the content of the chip in the card. Having the key and the card contents, they can put this information on blank cards and sell those in the streets. To the system those blank cards will look the same as the original card and people can travel on them. The only difference is the UID, but unless the system is designed with whitelists, which is not practical for systems with many cards (see below), the system has no way to tell that it is the UID of a card that is not part of the AFC system.

Alternatively, hackers could on the Internet publish software and the key to allow everyone who has a reader (which can be obtained for less than $25) to update the balance on their own legitimate cards.

2.2 No update mechanism for keys

Imagine again an Automatic Fare Collection (AFC) system in a city. Let’s assume this time that all keys in all cards are different and derived from encrypting the UID and other information by a master key (as explained in 3.1 below).

Now imagine that a criminal organization is able to obtain the master key by bribery or by attacks on a stolen Secure Application Module (SAM, see 4.1 below), which, although in most systems having a very low chance of happening, cannot be ruled out. Note that the master key is not present in any chip which is normally in the hand of consumers, so a device with the master key first needs to be stolen before an attack can be started (and then the attack must also be successful). All of this makes is less likely than an attack on a card.

Imagine finally that this system has no way to update (renew) keys on cards that are already in the field. In that situation, the system is left in the same state as described above in which all keys are the same. Using the master key, hackers could for each card calculate the keys and deploy this as described above.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

3. Mitigation of attacks on card

This chapter discusses attacks on cards. Note that some terminal side attacks, once successful, enable certain attacks on cards. Those attacks are also considered in this chapter.

3.1 Key elements in designing secure systems that can mitigate attacks on cards

These are the key elements in designing secure systems:

1. Key diversification:
   With key diversification each card has a key or keyset which is different from each other card.
2. Fraud detection:
   The ability to find out that a fraudulent card exists.
3. Mechanism to stop deployment of fraudulent cards:
   This can be either or both of:
   a. Black listing/ whitelisting:
      A mechanism by which the terminals can be instructed to accept or reject certain cards.
   b. MAC over the to-be-protected card contents and UID.
      Calculate a MAC over the card content including the UID and use a key for the MAC that is not present on the card (only present in terminals).
4. Key renewal:
   With key renewal the system has the ability to update the keys in the cards in the field, and use those new keys by the terminals. When a consumer presents a card that holds old keys, the keys will be updated to a new set of keys, and then the transaction will be performed.

We will discuss these concepts below. First some terminology though, followed by an overview of the effectiveness of the various defenses.

3.2 Terminology

Every MIFARE DESFire and MIFARE Plus has an ID. This is either a unique ID (**UID**) (meaning that there are no two genuine MIFARE cards that have the same UID) or in other cases an ID which is likely to be different from IDs of other cards by a high likelihood. In the case of non-unique IDs the likelihood of being able to acquire another card with the same ID as one that an attacker has access to, or even the ability to acquire two cards with the same ID is so low that it is negligible small for a commercially viable criminal business case. Therefore, we treat the non-unique IDs in this document as if they were unique IDs.

3.3 Overview of effectiveness

See Table 1 for an overview of the effectiveness of five sets of mitigation measures. The mitigation measures are discussed in more detail thereafter.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Table 1. Overview of effectiveness of the mitigation measures

#	Mitigation measures	Attack Deployment using the attacked card	Attacked Deployment using other legitimate cards of the system	Attack Deployment using new blank genuine cards	Attack Deployment via emulators
1	Key diversification	No protection	Effective protection (regardless of fraud detection) as long as the master key for key diversification in the terminal is not compromised.	Effective protection (regardless of fraud detection) as long as the master key for key diversification in the terminal is not compromised.	No protection
2	Key diversification + fraud detection + black/whitelisting	Effective protection from the moment of updating the black/whitelist	Effective protection (regardless of fraud detection) as long as the master key for key diversification in the terminal is not compromised. Otherwise: effective protection from the moment of updating the black/whitelist	Effective protection (regardless of fraud detection) as long as the master key for key diversification in the terminal is not compromised Otherwise: effective protection from the moment of updating the black/whitelist	Effective protection from the moment of updating the black/whitelist. If the master key for key diversification in the terminal would get compromized then the protection is not effective.
3	Key diversification + MAC over the UID and content	Partially effective protection. Residual risk: card can be brought back into a previously valid state of that card. Effectiveness: Not possible to put any value on the card, but only previously valid states. This holds as long as the key used in the terminal for the MAC is not compromised. When that key has been compromised: no protection.	Effective protection (regardless of fraud detection) as long as neither the master key for key diversification in the terminal nor the key in the terminal for the MAC calculation is compromised. When the master key for key diversification has been compromised: partly effective protection, see “Deployment using the attacked card”. When the key in the terminal for the MAC has been compromised: see row 1 above.	Effective protection (regardless of fraud detection) as long as neither the master key for key diversification in the terminal nor the key in the terminal for the MAC is not compromised. When only the master key for key diversification has been compromised: still effective protection. When only the key in the terminal for MAC has been compromised: still effective protection When both keys the terminal have been compromised: see row 1 above.	Partly effective protection. Residual risk: A previously valid state of the attacked card can be put on multiple instances of emulators. Effectiveness: Not possible to put any value on the card, but only previously valid states. This holds as long as the key used in the terminal for the MAC is not compromised. When that key has been compromised: no protection.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

#	Mitigation measures	Attack Deployment using the attacked card	Attacked Deployment using other legitimate cards of the system	Attack Deployment using new blank genuine cards	Attack Deployment via emulators
4	Key diversification + fraud detection + black/whitelisting + MAC over the UID and content	See 3 above until the moment that the black/whitelist has been updated, thereafter see row 2.	See row 3 above.	See row 3 above.	See 3 above until the moment that the black/whitelist has been updated, thereafter see row 2.
5	Methods 2, 3 or 4 with additionally the ability to do key renewal in the field.	Before updating the keys: same as in the original method. After a terminal key has been broken and this card is presented to an updating terminal, the original protection is regained. (This only holds if the keys for updating had not been compromised as well or if the updating transaction cannot be recorded by an attacker). For cards that are never presented to an updating terminal, original protection is regained once cards with keys derived from the compromised master key are no longer accepted.	Before updating the keys: same as in the original method. After a terminal key has been broken and this card is presented to an updating terminal, the original protection is regained. For cards that are never presented to an updating terminal, original protection is regained once cards with keys derived from the compromised master key/ MACs calculated with the compromised MAC key are no longer accepted by non-updating terminals.	Before updating the keys: same as in the original method. After a terminal key has been broken and this card (being a fraudulent card) is presented to an updating terminal, the updating of the keys will fail. That means that fraudulent cards cannot pass updating terminals. This event can also lead to blacklisting (in methods 2 and 4). Finally, full original protection is regained once cards with keys derived from the compromised master key / MACs calculated with the compromised MAC key are no longer accepted by non-updating terminals.	The same holds as for new blank genuine cards.

3.4 Key diversification

The principle of key diversification is that no two cards will hold the same key or keyset. Every card has a UID and this UID can be used to determine the key / keyset to be used.

Except for the smallest systems, it is unpractical for the terminal to hold a list of all the keys / keysets of all cards. Hence the key / keysets must be calculated from the UID. This is normally done by a process as illustrated in Fig 1.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

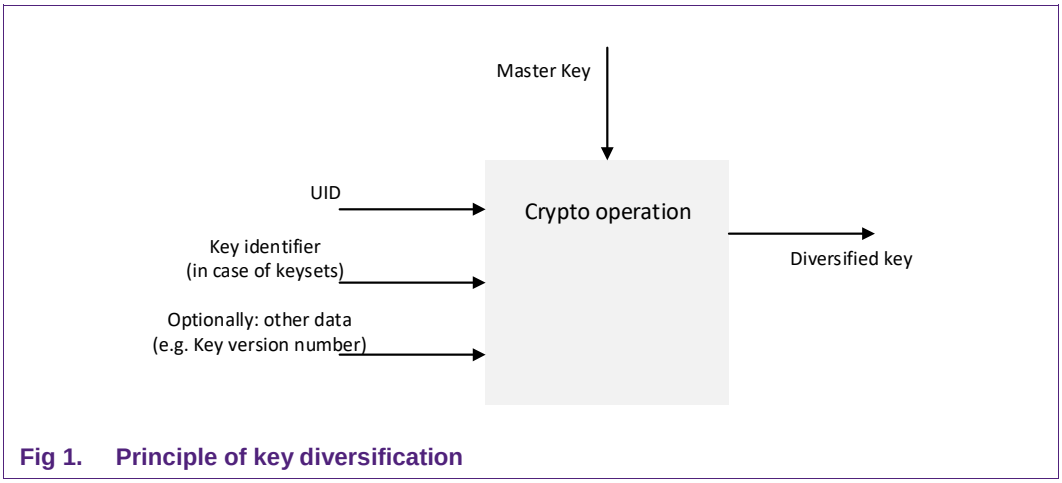

Fig 1. Principle of key diversification

The terminal holds a Master Key. The UID and other information concatenated and encrypted and the result is the diversified key. There are various cryptographic ways to do the key diversification operation. See [2] for the ways that the MIFARE SAM (Secure Application Module) performs key diversification. Even if your system does not deploy SAMs at the moment, it can be beneficial to use the same algorithm as the SAMs do, since this algorithm has been cryptographically verified, and it allows introducing SAMs later without having to change the keys on the card.

If each card holds a keyset (consisting of multiple keys for multiple purposes), the process in Fig 1 is carried out for each of those keys in the keyset (except e.g. a key to retrieve the UID, see 5.4).

The resulting key/ keyset is written on the cards during the personalization step, after the personalization station has read out the UID of the card.

The terminal first reads the UID and then calculates the diversified key / keyset it needs for the operation. Then this key/ keyset is used to set up the secure communication to the card.

3.5 Fraud detection

There are many ways of fraud detection which we cannot discuss here in any detail. In general it will come down to bringing together all transaction logs from all terminals and then detecting anomalies. Examples include: cards which suddenly get a higher balance without having been recharged with a value, cards which are used at two places within a time that does not allow for physical transportation of the cards between those places. Various system integrators have developed a variety of sophisticated algorithms for this.

Alternatively, when fraud becomes massive then it will become known. When fraud becomes massive then many people are involved and it is unlikely that no information will leak out.

3.6 Blacklists/whitelists

When blacklists or whitelists are used, the terminals are designed to hold a list with either all UIDs that are authorized for the system (in case of whitelisting) or all UIDs which have to be blocked (in case of blacklisting) or a combination of both.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

The system of whitelisting is more restrictive. However it is only usable in small systems. In larger systems, e.g. in an AFC system with millions of cards a whitelisting system would lead to an amount of data that terminals cannot handle.

The blacklists or whitelists must be updated after fraud has been detected. Terminals which are online can receive this information immediately after detection. Terminals which are normally off line must be put online at some time (e.g. terminals in busses get updated when the bus gets into the garage). Alternatively blacklists and whitelists can be distributed via other media, e.g. in a hotel the updates for the lists can be coded on the guest cards and be taken over by the terminal in the door when the guest presents the card.

A blacklist or whitelist system can be complemented with an “alarmlist”. This list will have UIDs which should trigger an alarm. Not only will the terminal potentially block the operation, but it will also give an alarm, e.g. to a guard who can arrest the fraudster.

3.7 MAC over content and UID

A MAC is short for Message Authentication Code. It is a cryptographic calculation over, in this case, the data on the card that is to be protected concatenated with the UID of the card. This MAC is calculated by the terminal and the result is written onto the card.

When a terminal gets presented a card, it reads all the relevant data as well as the UID and the MAC. It will first calculate a MAC over the relevant data and the UID and compare the result with the MAC that was read from the card. If they do not match the terminal will block the operation and could trigger an alarm if so desired.

The key which is used for the MAC calculation can also be a diversified key. It does not harm, however the importance of it is less than with the keys on the card. When an attacker would even be able to obtain all data and the MAC, a good MAC algorithm has as property that it is impossible to derive the key from those pieces of data. If a diversified key is used, then in the terminal the point of attack will not be the diversified key used for the MAC, but the master key from which the diversified key is calculated. When that is obtained, the attacker can himself calculate all required diversified keys.

3.8 Key renewal in the field

Both MIFARE Plus and MIFARE DESFire have the ability to do updating of keys on cards which are deployed towards the users of the system already.

The terminal will authenticate with an appropriate key in the card (which key depends on the access rights and how the system has been further set up). Then the terminal can write a new key or set of keys in the card.

We assume here that the keys used for updating in the card have not been compromised or that the updating messages cannot be recorded. If that were not true, the attacker could learn the new key.

When a master key used for key diversification would have been compromised (see 4.1 for ways to make compromising of master keys very unlikely), a new master key could be generated and deployed to all terminals. To a limited number of terminals, let’s call them the **updating terminals**, also the master key for updating of the keys in the cards would be deployed. Terminals in vulnerable environments will not get the keys to update keys in the cards, these are called **non-updating terminals**.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

When a user presents his card to the updating terminal, the terminal will read out the version number of the key/keyset used in the card and based on this first update the keys in the card to the keys for this card derived from the new master key. After this has been done the normal transaction, e.g. opening of the gate, would take place.

All considerations for key renewal are more complex than can be explained in this document. However one element is to take care of is the time of the total transaction, so the key updating plus the normal transaction, so that the user is not experiencing so much delay that he will think that the card does not work and removes it from the terminal to try again.

Note that any fraudulent modifications made to a card between the moment that a key is compromised and the moment that the keyset has been renewed are not undone by the key renewal and they have to be separately taken care of.

When a MAC key is compromised and has to be updated there is no special interaction with the card needed. The transaction will verify the MAC with the old key and compute the new MAC with the new key. It is recommended though that somewhere on the card there is a version indication of the key that is used for the MAC so that immediately the right one can be chosen.

After an update period the compromised master key for key derivation / the compromised key for MAC calculation is no longer deployed. This means that cards which have not passed an updating terminal will be rejected by other terminals and the user has to be told to first update his card in an updating terminal.

3.9 How the countermeasures help to mitigate the risks

Table 1 describes the mitigation measures.

Row #1: Key diversification only.

If only key diversification is used the impact of attacks is already strongly reduced. Since the key that is obtained is only valid for cards with the same UID, it needs either the originally attacked card or an emulator for the attack to be successfully deployed. Sending out the key and attack software to a wide set of recipients to modify their own legitimate card is countered by this measure.

This of course only works as long as the master key for key diversification is not compromised, since when an attacker has this master key then he can compute the keys for each card himself.

Row #2: Key diversification, fraud detection and black/whitelisting.

If key diversification is used, then it is possible in a system with black/whitelisting to additionally exclude the fraudulent card or replicas thereof based on the UID from the moment that the black/whitelist is updated.

Since due to key diversification the compromised key is only usable with a card or emulator with the same UID, the blocking of the UID guarantees that the attack is countered.

If the master key for key diversification were compromised, then the deployment of a fraudulent card is only blocked from the moment that the black/ whitelist is updated.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

However when the attacker uses an emulator, he can just choose another UID and calculate the keys for that card using the compromised master key. The fraud will continue in that case.

Row #3: Key diversification and MAC over UID and content.

In case a fraud detection and/or black/whitelisting system cannot be implemented, the usage of MAC over the combination of sensitive content and the UID can still provide a level of protection.

In this case, key diversification makes sure that only the original card or emulators can be used to deploy the attack, since the compromised key will only work if the UID is the same.

It is possible to revert the card back to a previously valid state by writing back that data plus the MAC which was then valid. And this can be done on the originally attacked card as well as on emulators that emulate the same UID, of which there can of course exist many copies.

It is not possible to put any desired value on the card, since then the MAC would fail.

If the master keys for key diversification would be compromised, the attacker can calculate the keys for all other cards based on the UID. So then any card can be brought back to a previously valid state and deployment via an emulator is possible. However introducing new cards with new UIDs is not possible, since there is no “previously valid state” for such cards, since they have never been in the system before.

If the key for the MAC calculation were compromised, the MAC is no longer effective and the system would be equal to a system with key diversification only as described in row 1.

Row #4: Key diversification, fraud detection, black/whitelisting and MAC over UID and content.

When combining #2 and #3, the combined benefits can be obtained.

Row #5: The other methods extended with key renewal in the field.

As long as no keys have been updated, the effectiveness is as in the original method.

The new master key or key for MAC is first deployed into all terminals, in addition to the old one, so that all terminals can deal with both old (not yet updated) and new cards (with updated keys).

If the keys on the card need to be updated, the updating terminals will in addition have the master key to derive the card update keys[1] from. These are the (again diversified) keys which are needed to update a key on the card.

When a card is presented to an updating terminal, it will update the keys and only then perform the transaction using the new keys. From that moment the protection for that card is in effect again.

When a card is presented with a UID which does not belong to the system, the authentication with the key update key will fail, since such cards do not have the right key update key. All updating terminals will then not let the transaction take place. The system could base on the failure to update the keys blacklist the card and deploy that blacklist also to non-updating terminals.

[1] The card update keys are the (diversified) keys, which are needed to change all other keys: this is the “ChangeKey key” for DESFire, or the “key B” for MIFARE Plus.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

For emulators the same holds in principle, however emulators can at no cost assume another UID and would then work again with non-updating terminals. Emulators will finally be stopped once the compromised key is no longer deployed to the non-updating terminals.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4. Mitigation of attacks on terminals

When the cards are properly protected using the methods described above, there are still attacks on terminals to take care of.

The terminals need to hold the master key or master keys from which the diversified keys are computed. When a master key becomes compromised then an attacker can calculate all diversified keys of all cards.

Below some methods are discussed to mitigate attacks on terminals.

4.1 Usage of a Secure Application Module (SAM)

The terminal must protect the master keys. A Secure Application Module (SAM) can hold keys and can on request perform cryptographic operations using those master keys, however not hand out the master keys themselves, nor the diversified keys.

If an attacker would steal and reverse engineer a terminal, then he may be able to use the SAM to change the data on a card, but cannot extract the key to deploy this key on other equipment. And the SAM can be configured to have an upper limit on the number of operations that it can perform using the master key until it has to re-sync with the backend, which will not happen of course once the theft has been detected and the SAM got blacklisted in the backend system.

Furthermore, the SAM can be configured such that it needs to authenticate itself towards the backend after power up. This means that an attacker who would steal the terminal and would drop power cannot use the SAM to modify cards.

The MIFARE SAM is a chip that is designed to withstand a multitude of attacks. For this chip the same considerations regarding strengths of attacks holds as described before for the cards. However the complexity of attacking a SAM is even higher than for the MIFARE cards. Where the MIFARE cards that belong the system, e.g. in the case of AFC, can just be bought from the AFC operator in a large quantity (since it is sold to the general public), in case of the SAM every SAM needs first to be stolen from a terminal. Attacks where multiple devices are needed will hence be very complicated.

4.2 Use different master keys for different purposes

It can be that there are different types of terminals which can / need to be protected differently.

Let’s assume an AFC system which has a great number of terminals placed at unmonitored platforms in train stations. Those terminals will only decrease the balance on the card.

The system also has (many fewer) terminals placed in buildings where they are monitored. Those terminals are used to increase the balance on the cards, e.g. in transactions that take the users credit card.

In such a system cards could be configured to allow decrementing the balance with one key and increment the value using another key (e.g. on MIFARE Plus X using value operations). In this case each card has a keyset consisting of two keys. Each of those two keys is derived from a different master key using (at least) the UID. The master key that is used to derive the diversified keys for the incrementing operation is only deployed to the terminals that are monitored.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

If an unmonitored terminal on a platform were stolen and reverse engineered and if a master key would be extracted, then this key can only be used for decrementing operations, which are not commercially attractive.

The master key which is used to derive keys for the incrementing operation receives in this setup an extra layer of protection by being in monitored locations and potentially also by more tamper resistance of the terminals in which they are deployed. A higher level of tamper protection can be affordable because of the lower amount of those terminals used for incrementing.

Finally it is good to have the master keys for updates of the keys/keysets to be different from the keys used for normal operation. Those master keys for updating would only have to be deployed in the field during a period of updating of keys, and only to a selected set of terminals where this updating takes place (the updating terminals).

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

5. What else is there to consider for designing a secure system?

Although MIFARE DESFire EV2 and MIFARE Plus EV1 have been tested as part of their CC EAL5+ certification to be able to withstand attacks that make millions of traces of interactions with the card, it is wise to limit unusual behavior. E.g. if the same card is interacting with a terminal it is OK to accept several tens of failed authentications, which would be a legitimate case if someone moves a card slowly towards the terminal. However if many more failed authentications occur it is good practice for the terminal to stop the interaction with the card and at least log the event.

This is only one of the examples of dealing with unusual behavior.

5.1 Checking of MACs

Request and check MACs that are used in the communication between the terminal and the card. Separate information is available on security considerations for the communication with the cards.

5.2 Relay attacks

MIFARE Plus EV1 and MIFARE DESFire EV2 supports proximity detection, which can be used to counter relay attacks. In relay attacks the communication between a legitimate card and a legitimate terminal is relayed between the card on a distance (e.g. in another country) and the terminal. If proximity detection is not implemented then such an attack is likely to succeed. If proximity detection is implemented then the attack will fail if the distance is beyond a certain minimum limit. Also here it is important to limit the amount of trials that card can make with a certain terminal by letting the terminal refuse to interact with the card after a number (multiple tens) of failed authentications.

See the documentation of MIFARE Plus and MIFARE DESFire [3] for further information.

5.3 Privacy

Privacy is a concern among several user communities. MIFARE Plus and MIFARE DESFire have several privacy protection mechanisms, one of them being the use of Random ID in the anti-collision process. See further the documentation of the respective chips.

5.4 Backend security

As said in the beginning of this document, the security that goes beyond the terminal is out of scope for this document. Those security threats include among others:

1. The software integrity in the terminals. If an attacker is capable to download fraudulent software into the terminal he could let the terminal open the gate if a card out of a certain set is presented without lowering the balance on the card.
2. Communication between terminal and backend. If an attacker can e.g. modify the blacklists or whitelists then this affects the security of the system.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

5.5 Withholding the CommitTransaction command

A generic threat to a (contactless) card system implementing a transaction mechanism can be the withholding of the final command of a valid transaction (in case of MIFARE DESFire the CommitTransaction command).

At the end of the valid transaction between reader and card, the attacker records and withholds the CommitTransaction command with a relay device. The card is also constantly kept on power using the relay device, meaning the session is kept open. The attacker can then decide whether to forward the command to the card to complete the transaction (e.g. in case of being inspected on a train or other means of public transport), or to power off the card and discard the transaction.

- In case the attacker was not inspected and decides to power off the card, the transaction is discarded and the card is not updated. The reader and / or backend would suspect that a tearing-event happened and the card was removed accidentally by the user too early from the terminal.
- In case the attacker was inspected, he can finish the transaction successfully by sending the withheld command to the card. The card will be updated and during the inspection, the card will appear as it was genuinely updated.

By executing this kind of attack, somebody could get illegitimate access to any service like e.g. public transit. Withholding of the final command is possible, as ISO/IEC 14443 allows the smartcard to be powered of infinite time without time-out between sending a response and receiving the next command. There`s no specific timeout value for this scenario defined in the standard.

Several precautions and mitigations can be taken on reader and system side, to prevent the described attack scenario:

- For gated access systems, a policy of only opening the gate after the transaction was fully completed, can be implemented. Here the successful transaction needs to including the final response from the card (meaning CommitTransaction response being returned form MIFARE DESFire).
- Fraud detection by keeping the card value / relevant data also stored in the system`s backend and applying card black-listing in case of card value inconsistencies. Careful black-listing needs to be applied, not to blacklist non-attackers unintentionally.
- Keeping track of cards that stop the transaction after the CommitTransaction command (no response sent from card any more) and eventually black-list these cards after they stop the transaction at the same command step multiple times. Potential valid card tearing needs to be taken into account.
- Verify that the card data was updated correctly and consistent. This can be achieved by e.g. executing two transactions – the first one needs to complete and in the second transaction one can read out the data content that should have been written during the first transaction. Alternatively also only one transaction can be executed, where one write operation to a StandardData file is included at the beginning of the transaction. The fact that something has been

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

written to the card can help to keep track and eventually black-list cards that hold inconsistent data due to not completing transactions. Potential valid card tearing needs to be taken into account.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

6. Risk analysis

This document has described a set of design principles for systems using contactless cards. Which of those mechanisms shall be deployed in any system must be the result of a risk analysis, which involves per attack the likelihood, the impact and the cost to mitigate the attack.

This document does not give further guidelines on how to conduct such a risk analysis as it will be very different per system. However a few general remarks can be made:

1. Do not underestimate the damage that can come from attacks that get publicity, even if there is no criminal business case attached to it. It can lead to much effort being spent on countering the bad publicity, and furthermore customers may lose their confidence in the system.
2. Even though fraudulent cards can be disabled by placing them on blacklists, when many of such cards exist the blacklists may overflow or searching them may have a negative effect on the transaction speed.
3. Do not underestimate what attackers are capable of doing. Very impressive things have been achieved in the past. Attacks that require a lot of knowledge and/or very expensive must not be ruled out on beforehand. There is intensive knowledge exchange among attackers and it is exchanged via communities of hackers on the Internet.
   Some expensive equipment which may be ruled out as obtainable for a certain class of attackers can often be rented by the hour or is easily accessible at universities.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

7. References

[1] AN11302 End to end system security risk consideration for implementing MIFARE Classic; document number 1551xx

[2] AN10922 Symmetric key diversifications; document number 1653xx

[3] AN155010 End to end system security risk considerations for implementing contactless cards; document number 1550xx

[4] AN3630 MIFARE DESFire EV2 Features and Hints; document number 3630xx

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

8. Legal information

8.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

8.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However NXP Semiconductors does not give any representations or warranties expressed or implied as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect incidental punitive special or consequential damages (including - without limitation - lost profits lost savings business interruption costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence) warranty breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document including without limitation specifications and product descriptions at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed authorized or warranted to be suitable for use in life support life-critical or safety-critical systems or equipment nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default damage costs or problem which is based on any weakness or default in the customer's applications or products or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors its affiliates and their suppliers expressly disclaim all warranties whether express implied or statutory including but not limited to the implied warranties of non-infringement merchantability and fitness for a particular purpose. The entire risk as to the quality or arising out of the use or performance of this product remains with customer.

In no event shall NXP Semiconductors its affiliates or their suppliers be liable to customer for any special indirect consequential punitive or incidental damages (including without limitation damages for loss of business business interruption loss of use loss of data or information and the like) arising out the use of or inability to use the product whether or not based on tort (including negligence) strict liability breach of contract breach of warranty or any other theory even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation all damages referenced above and all direct or general damages) the entire liability of NXP Semiconductors its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations exclusions and disclaimers shall apply to the maximum extent permitted by applicable law even if any remedy fails of its essential purpose.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products..

8.3 Licenses

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

8.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE — is a trademark of NXP B.V.

MIFARE Classic — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

MIFARE DESFire — is a trademark of NXP B.V.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

MIFARE Ultralight — is a trademark of NXP B.V.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

9. Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.

© NXP B.V. 2020. **All rights reserved.**

For more information, visit: http://www.nxp.com

Date of release: 22 April 2020 **196521**

Document identifier: AN10969