I am **ROBOT**

Chip Implant Guide

Table of contents

Everything arrived?

After opening, please check the contents of the package for completeness. Piercers and doctors always have the necessary utensils on site, but it is still recommended to bring them with you. Please refrain from opening the inner package. Otherwise the piercer will not be able to use the non-sterile needle and may refuse the injection. If you have chosen a partner piercer and already paid for the procedure via our online store, you do not need to do anything more than make an appointment with the piercer of your choice on your own.

Please make sure that you present the invoice or delivery bill on site so that the partner piercer recognizes that the procedure has already been paid for.

- Minimum addition -
Disposable gloves (non-sterile) • Chip Implant
Waterproof plasters • Wound plasters • Disinfectant or disinfectant wipes • Mask • This Guide

In the case of promotions or special offers, the additional scope of delivery may vary. If something is missing, please contact us immediately at support@iamrobot.de. Later complaints we can unfortunately not consider.

Test implants / test coins and cards

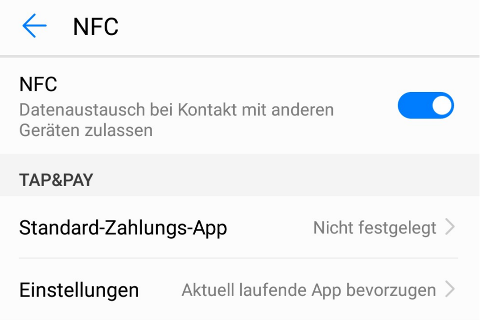
Thank you for purchasing a test implant! With this chip you can test your access control or smartphone final for compatibility. You can completely unpack and describe the test implant without this having any influence on the right of return.

Access control test (X1 / X2 / X3 / X4)

Make sure that the antenna or the external reader are switched on if they do not have an "auto wake-up" mode. Then slowly swipe the implant from one corner of the reader to the other. If the tag is rejected, the antenna can read those data that are reflected from the implant. For the X3 and X4 models, it may be necessary to format the implant in advance. You can perform the formatting, for example, with the "NFC Tools" app: To do so, select the "Other" tab and the "Formatting" option. Then slowly swipe the implant across the back of your smartphone until it vibrates and confirms the formatting. Now try to teach the implant to the system; just as you would do if, for example, a new transponder card is to be added. If this process works, it can be said with certainty that the respective terminal device is compatible with the implant.

Check smartphone (X2 / X3 / X4 / XRange)

Activate the NFC function of your smartphone. You can usually find this option on Android devices under Settings - More - NFC. Now install any NFC app from the Google App Store. We recommend the "NFC Tools" app for this purpose. To be able to read out the implant later - after "programming" - from any smartphone, no app is required. As soon as the NFC function is activated and you have installed a corresponding app, you can try to read in the implant. The NFC antenna is located in a different place on each smartphone. You may need several attempts to find the NFC hotspot. Note that thick smartphone cases may limit the reception of the implant. Try writing a record on the test implant when you have found the hotspot. If this process is also successful, your smartphone is fully compatible.



NFC

NFC
Datenaustausch bei Kontakt mit anderen Geräten zulassen

TAP&PAY

Standard-Zahlungs-App — Nicht festgelegt

Einstellungen — Aktuell laufende App bevorzugen

Warnings before use

Please read the instructions for our product carefully.

Our implants are sterile packed. Please check that the packaging is undamaged and that the paper inside has not become wet. If you have purchased an implant from the X-series, please check whether the inner packaging is still airtight.

Once the protective packaging has been opened, our product is excluded from exchange. Please open the packaging only shortly before the procedure. Premature opening increases the risk of infection of the puncture wound. In addition, piercers usually refuse the procedure if the sterility of the needle is limited. **The implant cannot be tagged and read in the syringe. The metal of the syringe prevents communication between the smartphone and the RFID antenna.** So this is not an indicator that the implant is not writable or even defective. Furthermore, you may not be able to read the implant immediately after the procedure. Please be patient for 3-7 days before contacting us. The patch and wound water have a significant impact on the connectivity of the implant.

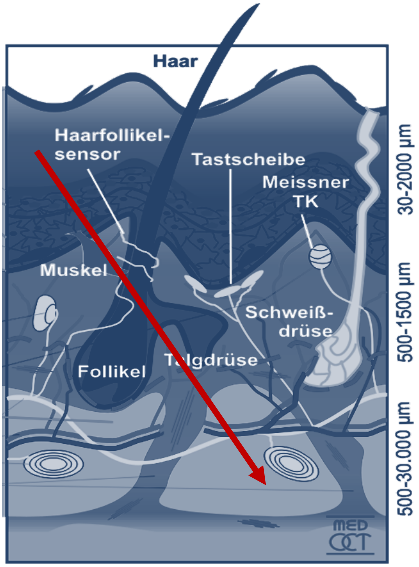
We strongly advise having the procedure performed by professionals. Self-implantation can not only injure veins or muscle tissue, but there is also a greater risk of infection. Even if you have not purchased a procedure through our website, you can still use our partner piercers. However, we will only cover the cost of the procedure if you select "With procedure" in the online store. If we do not list a partner in your area, please contact us. We will do the search for you free of charge.

The use of the chip as an implant is entirely your own responsibility. Every body is different, as well as every piercer has his own style of placing piercings. These two factors are crucial for the future connectivity of the implant. As a result, the implant cannot be read by some compatible smartphones. Many NFC apps support the "lock" function. Please never select this option. Afterwards, you will no longer be able to write to your implant!

Implantation procedure

This is not a guide to self-implantation, but merely a guide for piercers and professionals to achieve the best possible result .

The implant is basically pierced like a surface piercing. This means that it is placed between the lower skin layer (subcutis) and the fatty tissue. Care must be taken not to injure the muscle tissue or veins. To ensure this, the forearm is grasped and the hand is successively clenched into a fist and released again. This will make larger veins visible. An LED flashlight shining through the first layers of skin can be helpful.

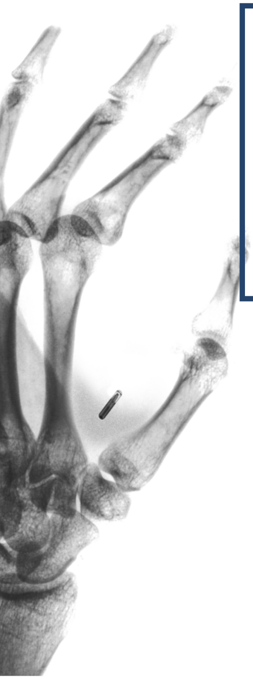


Usually, the implant is implanted between the thumb and index finger. This location has the advantages that, on the one hand, you can interact well with your hand - e.g., with smartphones or electronic door locks, and, on the other hand, the skin at this location is not particularly thick, so a good connection to smartphones can be established. Check whether the organic glass head is intact by removing the protective clip and the plastic sleeve. To do this, gently push the insertion plunger forward until approximately 1mm of the implant is visible. If the bio-glass dome is intact or obviously not damaged, you can start the implantation. Push the implant back into the needle with your disinfected glove so that the tip completely encloses the glass dome again.

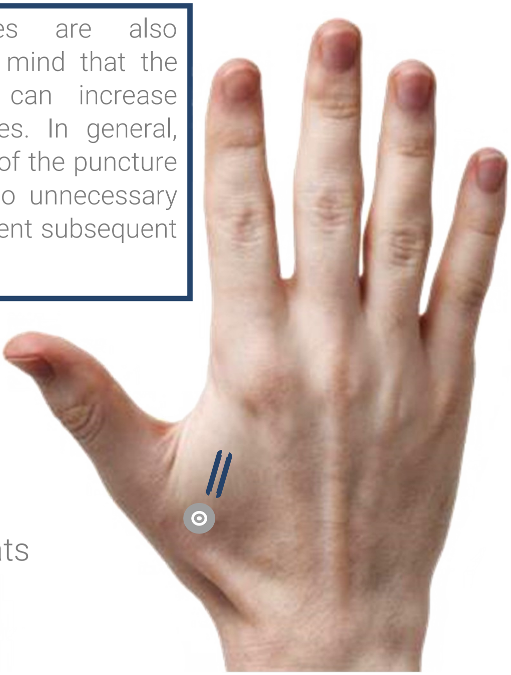
Implantation procedure

After you have ensured that veins and muscle tissue cannot be injured by the injection needle, use your index finger and thumb to grasp the fold of skin where the implant will later be placed. To prevent the implant from slipping off, make sure that you do not prick close to the bone or skin in the hollow between your thumb and index finger. Remember to remove the protective clip on the insertion plunger or it will not push in.

Penetrate at the lower point of the formed skin fold and push the injection needle about 10mm under the skin layer. Make sure that the longer side of the needle points downwards. Now push the insertion plunger completely and with some pressure into the injection device. Carefully pull the needle out and gently squeeze the puncture wound to prevent possible air entrapment. Then use our supplied wound plasters to protect the puncture wound from external influences. You should wear the plaster for at least two days and change it the following day.



Other implantation sites are also conceivable. Just bear in mind that the foreign body sensation can increase considerably at some sites. In general, after implantation, the site of the puncture should not be subjected to unnecessary stress in order to also prevent subsequent slipping of the implant.

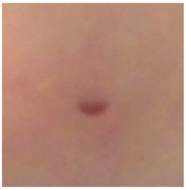


◎ Einstichpunkt

// Sitz des Implantats

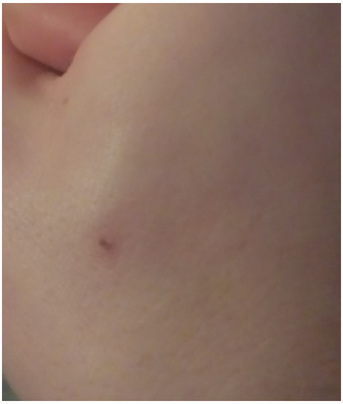
Healing process

The healing process presented here is based on customer testimonials and own experience. The healing can develop differently for everyone!



The first image was taken immediately after an NFC implantation. The approx. 2.5mm puncture wound is clearly visible. The wound is still open and bleeding a little. When showering, one of the waterproof plasters should definitely be worn.

The photos can be viewed here in larger resolution. You will be redirected to our website after scanning the code.



Due to a small swelling, minor numbness may occur in a radius of about 3cm around the puncture wound. The swelling goes down after the first few days, so that the "knocking" and numbness decrease. We strongly recommend not to move the implant under the skin yet.

The second picture was taken three weeks after implantation. The wound crust has almost completely disappeared. There are no longer any foreign body sensations. The NFC implant can no longer be felt, even with unusual hand movements. The healing process also includes scarring: When the crust has completely disappeared, a small scar of about 1-2mm remains, but it is hardly noticeable or not noticeable at all.

Technical details

Our implants have different features and chipsets. Each of them is tailored to specific applications, so that size, connectivity, chipset and use form a symbiosis. Here you will find a small technical overview of your implant.

Model	Chipset	Manufacturer	Memory	Writable	Frequency
X1	EM4100 EM4200 EM4305	EM Microelectronic	8Bytes 8Bytes 512Byte	- - 512Byte	125kHz (LF)
X2	NTAG216	NXP®	888Bytes	556Byte	13,56MHz (HF)
X3 / Elite	M1 Classic Fudan S50	NXP® Fudan	1024Byte 4096Byte	716Byte	13,56MHz (HF)
X4	DESFire	NXP®	2048Byte 4096Byte 8192Byte	2048Byte	13,56MHz (HF)
X Range	iCode Sli	NXP®	106Byte	106Byte	13,56MHz (HF)

Compatibility

There are different approaches to detect or interpret compatibility with existing devices. Most modern reading antennas, which are coupled to relays to open doors, for example, support MIFARE Classic® and compatible chips such as the Fudan S50. Older locking systems may well use the 125Khz frequency (X1). If you try to read in the transponder card using a smartphone (NFC Tools app), the app will show you the chipset that is being used. However, if the smartphone does not respond to the transponder, it is possibly 125kHz technology.

Read and write NFC implant (X2, X3, X4, Range)

Please note that you will not yet be able to scan the implant shortly after the procedure. The wound water and the plaster may be too great a resistance for the comparably weak NFC antenna of the smartphone. We recommend the "NFC Tools" app to get started, as it is easy to use, you don't need any prior knowledge and many free functions are supported. Scan the QR field or search for "NFC Tools" in the Google Play Store.

An NFC smartphone with an active NFC mode is required for reading. Depending on the manufacturer, the antenna, i.e. the battery, is installed at different heights. Therefore, it is a matter of practice to find the antenna. It is best to make a fist so that the implant is visible and slowly stroke the back of the smartphone from bottom to top. The slower you do this, the more accurate the localized spot will be for reading the implant in the future. Make sure that the smartphone has NFC and that this function must also be activated. In addition, there may be connectivity restrictions if you use a case. Please do not use the "Lock", "Encrypt" and "Secure with password" functions if you do not know exactly what they do. You may not be able to read or write to the implant completely afterwards. This is irreparable!

If you have let some time pass, the wound is no longer swollen and you cannot establish contact with your smartphone, please send us an email at support@iamrobot.de.

The NFC implant can no longer be read out.

Is NFC enabled? Does the energy-saving mode hinder the NFC function? Did you replace the battery with a replica or from a third-party manufacturer? Have you had the implant implanted in an unusual location? Has the implant been locked or password protected by the encryption function? Was the procedure performed less than 3 days ago? Does the scanning process not work with your smartphone only? Please contact us if you have answered all these questions in the negative - we are sure that we will find a solution. It is extremely unlikely that a malfunction of the implant will lead to a health hazard. However, if the malfunction is caused by a serious accident, the cylinder may have been damaged. To our knowledge, this has never happened before. In such a case, a doctor should be consulted immediately.

The NFC implant has slipped.

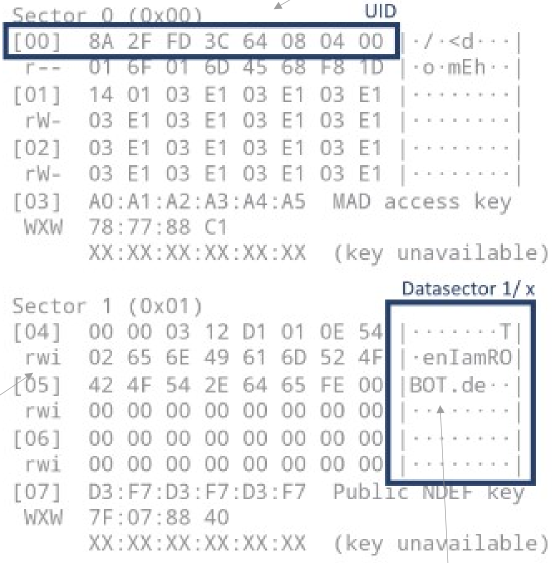
Our partner piercers record the subsequent position of the implant before the injection. If, after removing the wound plaster, you notice that it has slipped up or down, you should not try to move the implant by force - it may be that slight swelling pushes it slightly to the side. Once the wound has healed, it is possible to move the implant slightly. The optimal position is above the muscle of the ball of the thumb. If the thumb and index finger of the implant hand are pressed together, this muscle comes to the fore. When the implant sits on the upper part of the muscle, it has the best connectivity because the distance between the implant and the antenna is very small. However, if the implant slips all the way into the fold of skin between the thumb and index finger and there is even a foreign body sensation, you should have the implant removed and reinserted.

Functionality of an NFC implant (X2 and X3)

Chip implants, which include all RFID transponders such as the X1, are passive transponders without their own power source. This means that an active transponder is always required, i.e. an antenna that "irradiates" the implant and supplies it with energy. This small energy source is sufficient to read or write to an implant.

UID and records

The NFC implant consists of different sectors on which data can be stored. Sector 0 contains the UID, also known as the serial number (unique permanent identification). This is used, for example, to identify home automation systems, locking cylinders, etc. The serial number can be interpreted in a variety of ways (HEX). The serial number can be interpreted in various forms (HEX / DEZ) and is a fixed component of the chip. Sector 0 cannot usually be written to or manipulated. Further sectors with consecutive numbers follow. These blocks are writable and are used by apps and licenses to either personalize the chip or equip it with additional security features. The labeling on the left - "r" (read) "w" (write)" - indicates which blocks can only be read and which can also be written. Smartphones usually read blocks until a sector is recognized as an application; they then execute it.



```
Sector 0 (0x00)
[00]  8A 2F FD 3C 64 08 04 00 |·/·<d···|
 r--  01 6F 01 6D 45 68 F8 1D |·o·mEh··|
[01]  14 01 03 E1 03 E1 03 E1 |········|
 rW-  03 E1 03 E1 03 E1 03 E1 |········|
[02]  03 E1 03 E1 03 E1 03 E1 |········|
 rW-  03 E1 03 E1 03 E1 03 E1 |········|
[03]  A0:A1:A2:A3:A4:A5  MAD access key
 WXW  78:77:88 C1
      XX:XX:XX:XX:XX:XX  (key unavailable)

Sector 1 (0x01)
[04]  00 00 03 12 D1 01 0E 54 |·······T|
 rwi  02 65 6E 49 61 6D 52 4F |·enIamRO|
[05]  42 4F 54 2E 64 65 FE 00 |BOT.de··|
 rwi  00 00 00 00 00 00 00 00 |········|
[06]  00 00 00 00 00 00 00 00 |········|
 rwi  00 00 00 00 00 00 00 00 |········|
[07]  D3:F7:D3:F7:D3:F7  Public NDEF key
 WXW  7F:07:88 40
      XX:XX:XX:XX:XX:XX  (key unavailable)
```

Basically, you have two main functions at your disposal. One is the use of the UID and the other is the data memory, which can be written to according to your wishes using a smartphone or NFC writer.

The UID is a defined serial number that you can use to identify yourself (page 12). This opens up several application possibilities for you. In everyday life, numerous electronic identification procedures are based on a UID. It is not uncommon to already accomplish this using MIFARE® transponder cards or tags, which are nothing more than the UID on your NFC implant. In many cases, it is possible to replace or add to the already stored UID in access systems, as would be done if, for example, a transponder card or coin were lost or an additional user were added.

Application examples

Electronic locking cylinders • HID PC Login • Access control
locker systems • Membership cards • Tickets
NFC relays • Elevators • Electronic time stamps • Tripod barriers Service
passes • Parking garages • Gyms and many more

The UID - i.e. serial numbers - cannot be changed until further notice (X2,X3, X4, Range). This means that the main system must always teach the UID as a new transponder / member card and not vice versa. The UID of the transponders cannot be manipulated with original NXP® chipsets to simulate the already stored UID. The X3 Elite is the only exception to this. With this model, the UID can be changed to simulate an existing access card.

X3 Elite specifics and the UID serial number

The X3 Elite chipset takes advantage of a security vulnerability that allows sector 0, i.e. the UID of the chip, to be changed. With the software supplied, it is therefore possible to clone existing transponders such as RFID access cards and replace them with the X3 Elite implant. This makes a complicated exchange of the transponders obsolete.

UID in everyday life

The UID is used for authentication at terminal devices. In concrete terms, this means that a reading unit, such as an external antenna, picks up the UID or serial number of the respective transponder and forwards it. A controller then checks whether the serial number is granted access or rejected - if, for example, the UID is not known to the system. This procedure is very common in everyday life and has the benefit of checking quickly and efficiently whether the cardholder is authorized or not. This verification procedure can be found, for example, in electronic access controls in gyms, office buildings, at front doors, or as access controls for electronic time stamping, PC units, public transportation monthly passes, etc. The principle behind this technology is always the same.

The shortened way

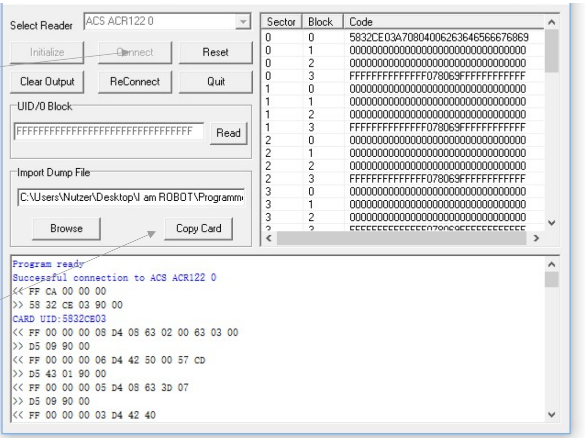
Since it was not possible to exchange or edit sector 0, the additional UID in the system that decides on access or entry had to be taught or exchanged, since the implant had to retain its fixed UID. Thus, with other implants, one is forced to teach a new "access card". The X3 Elite, on the other hand, has the unique feature of being able to memorize the serial number of the existing transponder, so that, for example, the turnstile in the gym or the access control system in the office starts from the original transponder and access is granted. The cloned UID can then of course also be taught to other systems.

Copying other people's access cards, e.g. to gain unauthorized access, is a criminal offense. Only use this function with your own transponders or with the express permission of the owner.

A smartcard reader is required to read and copy the transponder. We recommend the ACS U122. First check whether the transponder card or chip you want to clone is a MIFARE Classic chipset.

The easiest way to check this is to use the NFC Tools app. Then download the program "X3_Elite_Clone.rar" using the link sent to you and unpack it. Now plug in the ACS U122 and wait until the red lamp lights up. Now start the .exe "Step1_Image_create". Select the smartcard reader in the dropdown menu and place the transponder that is to be copied to the chip implant on the device so that the green lamp lights up continuously. Then click on the button on the right and wait until the UID is visible under the key matrix. You have created a "dumpfile", i.e. an image of the transponder. Now open the .exe "Step2_Image_copy" and proceed as follows:

Initialize the smartcard reader and place your hand on the reader so that the green dot lights up continuously. To avoid disconnections from the implant, it may help to make a fist. When you are ready, click "Connect." The X3 Elite implant is now read in and can be labeled. Now select the backup file you created earlier. Hold your hand on the smartcard reader again and click on "Copy Card".



Select Reader: ACS ACR122 0

UID/0 Block: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

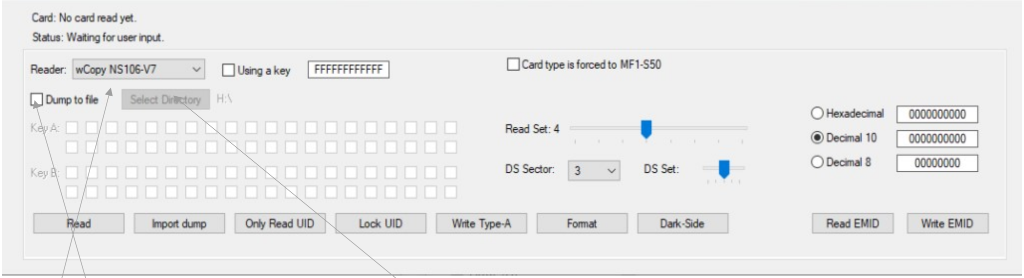
Import Dump File: C:\Users\Nutzer\Desktop\I am ROBOT\Programm

Sector	Block	Code
0	0	5832CE03A70804006263646566676869
0	1	00000000000000000000000000000000
0	2	00000000000000000000000000000000
0	3	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
1	0	00000000000000000000000000000000
1	1	00000000000000000000000000000000
1	2	00000000000000000000000000000000
1	3	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
2	0	00000000000000000000000000000000
2	1	00000000000000000000000000000000
2	2	00000000000000000000000000000000
2	3	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
3	0	00000000000000000000000000000000
3	1	00000000000000000000000000000000
3	2	00000000000000000000000000000000

```
Program ready
Successful connection to ACS ACR122 0
<< FF CA 00 00 00
>> 58 32 CE 03 90 00
CARD UID:5832CE03
<< FF 00 00 00 08 D4 08 63 02 00 63 03 00
>> D5 09 90 00
<< FF 00 00 00 06 D4 42 50 00 57 CD
>> D5 43 01 90 00
<< FF 00 00 00 05 D4 08 63 3D 07
>> D5 09 90 00
<< FF 00 00 00 03 D4 42 40
```

Clone transponder with the X3W Cloned Writer

Using our Writer is child's play. The program is specially tailored to it, so you only need a few clicks to create a dump (backup) and copy it to a writable chipset. To do this, connect the X3W Cloned Writer to a free USB port and open the drive. Start the program that is on the Writer.



Card: No card read yet.
Status: Waiting for user input.

Reader: wCopy NS106-V7
□ Using a key FFFFFFFFFFFF
□ Card type is forced to MF1-S50
□ Dump to file H:\
Read Set: 4
DS Sector: 3
DS Set:
○ Hexadecimal 0000000000
● Decimal 10 0000000000
○ Decimal 8 00000000

First check if the Writer is recognized by the program. If not, select the device manually using the drop-down menu. If you want to create a dump file, select the check box "Dump to File" and to the right of it the directory where the dump file should be saved. Now place the transponder that is to be copied on the Writer and confirm the process with "Read". When the process is complete, select the dump, uncheck the "Dump to file" checkbox and place the X3 Elite or other writable chipset on the Writer. When the Writer beeps briefly, the chipset has been detected and can be written to using the "Write Type-A" button. The Writer can also be used to format the chipset. On the right side of the program is the area where EM4200 can be copied to EM4305 transponders. Since EM4305 chipsets are freely writable ex works, the desired ID can be entered into the field. It will then be written to the X1 implant using the "Write EMID" button. If you want to read a transponder to check if the write process worked, you can do this with the button "Read EMID".

Many smartphone applications or programs, such as those presented on the previous page, offer the option of locking the UID or even the complete chipset. This is then actually locked and remains in this state, so that some functions - such as writing data records - are no longer possible! So don't use this function if you don't want to lock the chip.

The rest of the chipset is freely available to you. You can write to it, delete it, format it and read it. Various apps are available for this purpose. We recommend the app "NFC Tools" because it is free of charge, has a user-friendly structure and offers many features that are otherwise only available in paid apps.

If you have already familiarized yourself with page 10 of the guide, you have probably already tried out some of the app's functions. Data sets or executions are always recognized in the sectors by an input command, such as. "vcard". Regardless of whether the app "NFC Tools" has been installed, the smartphone recognizes this command when scanning the NFC implant and opens the "vcard", i.e. contact data that has been stored on the implant. If you use several data sets, the data set that was described first is always executed. If you want to use more functions at the same time, it makes sense to use "conditions" and "OR" functions with the Pro version.

Application examples

Business Cards • share Data • Dropbox Access Permissions
Bitcoin Interface • Emergency Data
Application Executions • Digital Will
Certificates • Memos • PayLink and more.

Privacy

The chip implant can be read by anyone. The only requirement is direct contact with an active antenna, such as a smartphone. It is not advisable to store data that is not intended for sharing. Alternatively, the chip implant can be encrypted, but this cryptography is considered insecure for sensitive data.

Your data in safe hands

NFC implants cannot be located or monitored. The chipsets do not have their own power source, so GPS modules or similar are not conceivable. Furthermore, the memory can be written to and formatted individually. The chip does not track any data, as is the case with smartphones, for example. RFID technology or especially NFC (Near-Field-Communication) have the property to share data only on short distances (~5cm). Due to the even smaller antenna used in chip implants, the range is severely limited. In addition, it should be noted that due to the small memory, "monitoring" would be rather uninteresting, since the data sets themselves are modifiable and the serial number cannot be assigned to any person. Reading data is therefore only possible with direct contact of an active antenna such as a smartphone. Only save data that is also intended for sharing.

Extension options

We offer upgrades on the hardware side. The UID presented earlier can be read by our antennas and forwarded to relays. The relay is able to close a circuit to control technical devices.

Access control Vehicle Electronics Electronic devices

All technical devices can be addressed and controlled potential-free or with a 12V potential. If you are unsure about end devices, we will be happy to help you with the installation via remote maintenance.

Technical support and contact

If you have any questions about chip implants and relay controls, please do not hesitate to contact us. In order to be able to process your request quickly, it is advantageous if you contact us via e-mail for technical questions or if you leave us a callback request with the respective topic. This way we can ensure that the right contact person is available for you and can handle your request professionally.

Mail addresses

General inquiries	support@iamrobot.de
Billing office	buchhaltung@iamrobot.de
Dealer inquiries and similar	s.becker@iamrobot.de

Phone
+49 231-58695638

Callback service
https://iamrobot.de/support/

I am ROBOT—UG haftungsbeschränkt
Chemnitzer Straße 126
44139 Dortmund
Germany