

# RFID für Maker

*Pi and More 12: 16.11.2019*

RFID / NFC Standards kennen und  
in Projekten nutzen

# Über mich

- › Tobias Blum
- › Aus der Nähe von Saarbrücken
- › Studium: Angewandte Informatik in Zweibrücken
- › Hauptberuflich: Senior Webdeveloper bei netmedia.de
- › Vortrag auf der Pi and More 9:  
„Ein SmartLight im Selbstbau für unter 15 €“  
<https://github.com/toblum/McLighting/>
- › Vortrag auf der Pi and More 10:  
„Software Defined Radio – mit dem Pi per ADS-B den Luftraum in der Großregion beobachten“
- › Vortrag auf der Pi and More 11:  
„SmartHome Hacks aus der Praxis“

# Übersicht

- › Was ist RFID (und NFC) eigentlich?
- › Wie funktioniert das?
- › Welche Standards gibt es?
- › Howto: Tags mit dem Smartphone auslesen
- › RFID Hardware für Maker
- › RFID im eigenen Projekt: Arduino / Raspberry
- › Projektbeispiel: ESP-RFID Access Control System
- › Projektbeispiel: RFID fähiger MP3 Player

Was ist RFID  
eigentlich?

# Was ist RFID eigentlich?

- › Wikipedia sagt dazu:
  - „RFID (englisch *radio-frequency identification* ['ʒeɪdɪəʊ  
'fʃi:kwənsi aɪ dɛntɪfɪ'keɪʃn] „Identifizierung mit Hilfe elektromagnetischer Wellen“) bezeichnet eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.“
- › Ein RFID-System besteht aus:
  - Einem Transponder (Funketikett, Tag, ...)
  - Lesegerät

# Einsatzzwecke

- › Ausweise: Seit 2005 in Reisepässen, seit 2010 in Ausweisen.
- › EC / Kreditkarten
- › Fahrzeugidentifikation: In UK im Feldversuch auf Nummernschildern, in US und CA auf Waggonen / Lokomotiven.
- › Tieridentifikation: Als Implantat (ISO 134,2 kHz)
- › Medikamente als Echtheitsnachweis
- › Textilien / Bekleidung: z.B. Levis, C&A (2012), Decathlon (2013)
- › Wegfahrsperre am Auto: Crypto Transponder im Schlüssel
- › Zutrittskontrolle / Zeiterfassung / Eintrittskarten
- › Mülltonnen: Für Müllmesssysteme / Abrechnung

## Und was ist NFC?

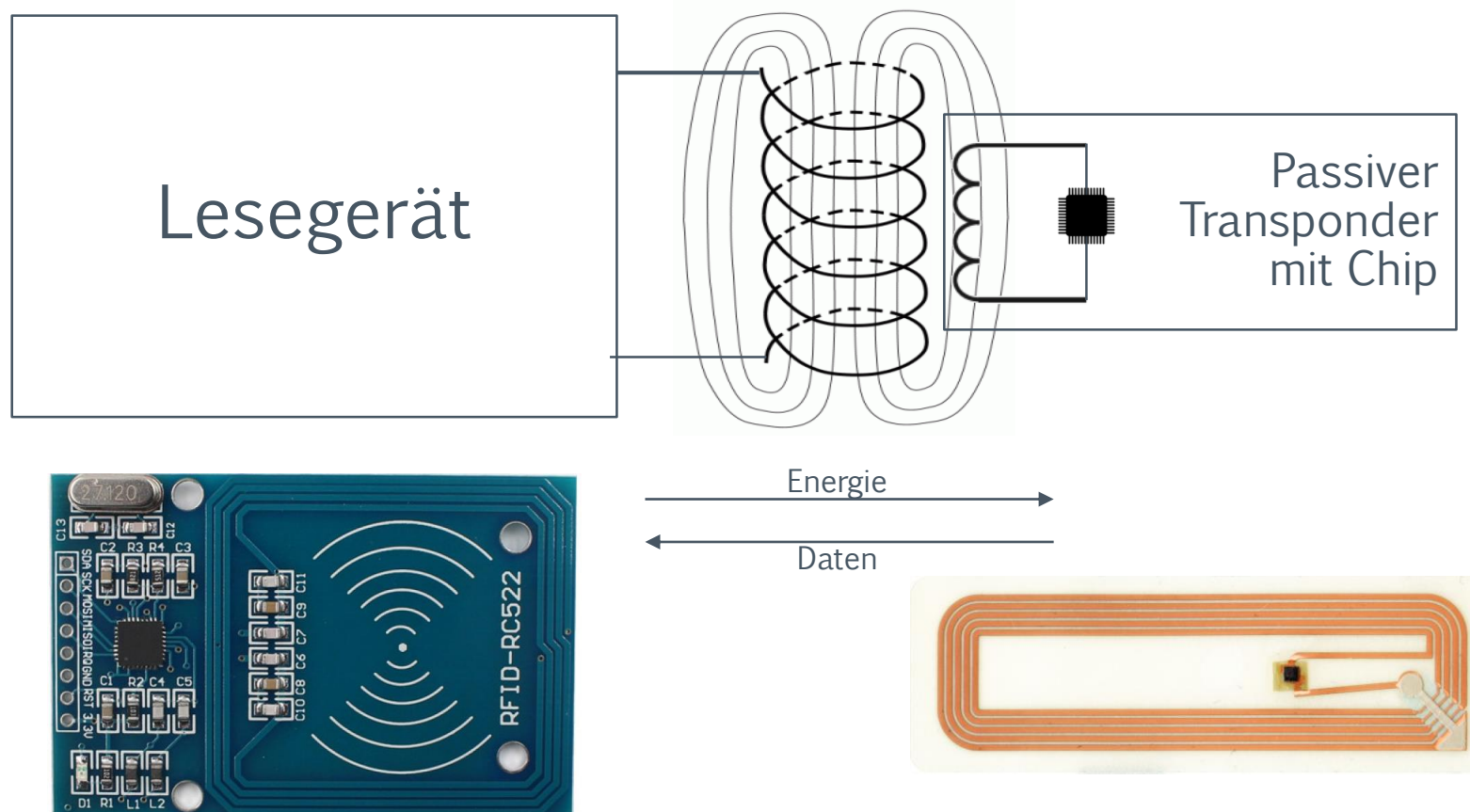
- › Wikipedia: „Die Near Field Communication (dt. Nahfeldkommunikation, abgekürzt NFC) ist ein auf der RFID-Technik basierender internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten ...“
- › Arbeitet mit 13,56 MHz mit Karten nach ISO14443A
- › Dahinter steht das NFC Forum, gegründet 2002 von Philips (später NXP) und Sony.
- › Erste Spezifikation 2006, erstes Gerät Nokia 6131.
- › 2009: Standards (NDEF) für Übertragung von Kontakten, URLs

Wie funktioniert  
das?



# Wie funktioniert das?

## Passiver Transponder



Welche Standards  
gibt es?

# Welche Standards gibt es?

## – Frequenzen

- › Langwellen (LF, 30–500 kHz),  $\leq 1$  m Reichweite, häufig in der Industrie, aber auch Wegfahrsperren, Zugangskontrolle (125 kHz), Tier-Identifizierung.
- › Kurzwellen (HF, 3–30 MHz),  $< 10$  cm Reichweite günstige Transponder/Lesegeräte SmartTags (13,56 MHz)
- › Sehr hohe Frequenzen (UHF, 433 MHz ([USA](#), [DoD](#)), 850–950 MHz ([EPC](#) und andere)), 2–6 m Reichweite für passive Transponder, hohe Lesegeschwindigkeit, sehr günstig, häufig zum Warenmanagement auf Containern, Paletten, Produkten, auf Autokennzeichen (UK), Kleidung
- › Mikrowellen-Frequenzen (SHF, 2,4–2,5 GHz, 5,8 GHz und darüber), 0,5 m bis 6 m Reichweite, nur semi-aktive Transponder, hohe Passagegeschwindigkeit, daher oft auf PKWs in Parkhäusern, Waggonen, Mautstationen, ...

# Welche Standards gibt es?

- Unzählige Standards je nach Anwendungsfall
  - › <https://de.wikipedia.org/wiki/RFID#Normen>
- Mifare
  - › Mifare von NXP Semiconductors (ISO 7816 bzw. ISO 14443A) ist die vermutlich meistgenutzte Technik (bisher > 10 Mrd. Tags verkauft)
  - › Arbeitet mit 13,561 MHz, Reichweite bis zu 10 cm, passiv
  - › MIFARE Classic 1K (720 Bytes)/4K (3360 Bytes)
    - Verschlüsselung implementiert, aber seit 2008 geknackt.
  - › Nachfolger:
    - Ultralight (LowCost für Fahrscheine, ...), Ultralight C (mit 3DES Crypto)
    - Classic Plus S (wie Classic, aber mit AES 128 Crypto)
    - DESFire (Microcontrollerbasierend, 3DES)
    - ...

# Die Mifare Classic Card 1K

- 1024 Bytes Speicher verteilt auf 16 Sektoren mit jew. 4 Blöcken
- Geschützt mit zwei Schlüsseln (Key A und B)
- Die ersten 16 Bytes enthalten Herstellerdaten und die eindeutige UUID und sind Read-Only
- 16 Bytes jedes Sektors sind für Keys und Zugriffsregeln reserviert
- UUID 4 Bytes (selten auch 7 Bytes) und werden nicht zentral vergeben, damit sind Duplikate denkbar.
- Es verbleiben somit 752 Bytes netto zum Beschreiben.
- Können dauerhaft „fixiert“ werden.

# Der NDEF Standard

- Gängiger freier Standard für Datenaustausch per NFC.
- [http://www.nfc-forum.org/specs/spec\\_list/](http://www.nfc-forum.org/specs/spec_list/)
- Unterstützte Karten, z.B. Mifare Classic / Ultralight können als NDEF Karten formatiert werden (manchmal bereits so formatiert ausgeliefert) und dann beschreiben werden.
- Unterstützung für versch. Datentypen:
  - › URLs, Text, Mail, Kontakt, Telefonnummer, SMS, Ort, WLAN Netzwerk, Bluetooth Verbindung, Adresse, freie Daten
- Das Lesegerät entscheidet, wie es die versch. Datentypen interpretiert / öffnet

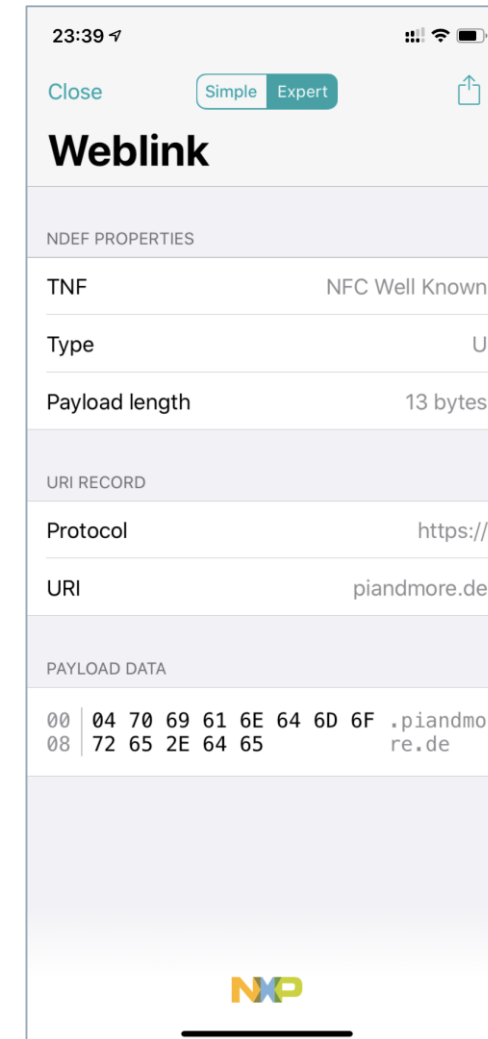
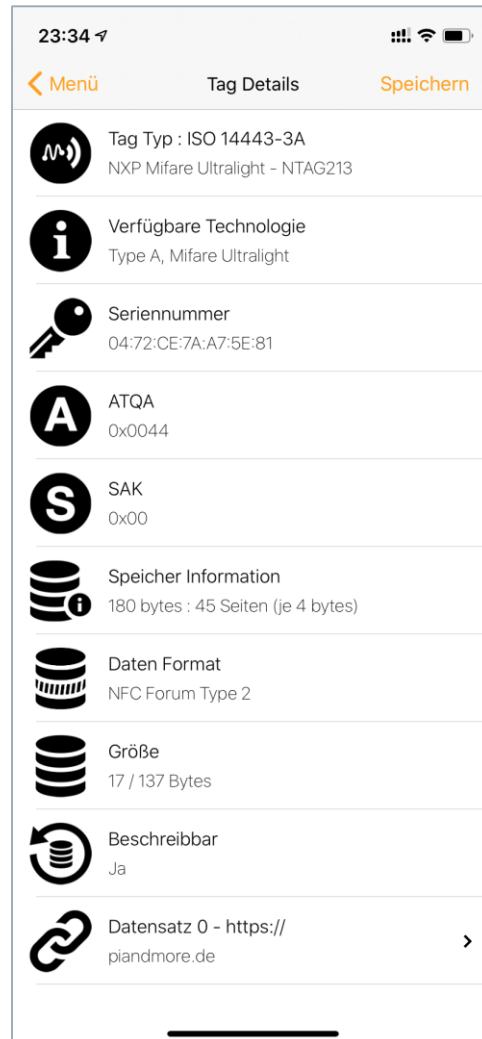
Tags mit dem  
Smartphone lesen

## ›Howto: Tags mit dem Smartphone auslesen

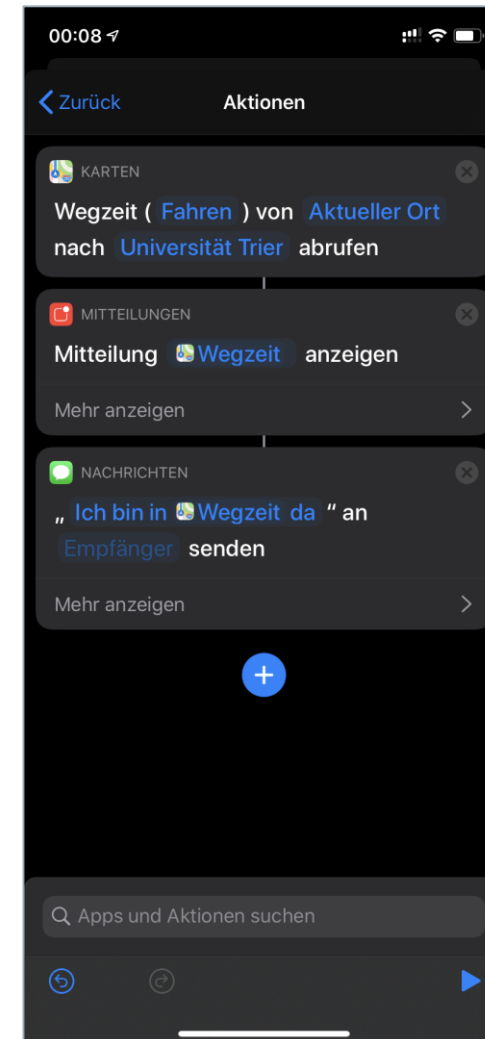
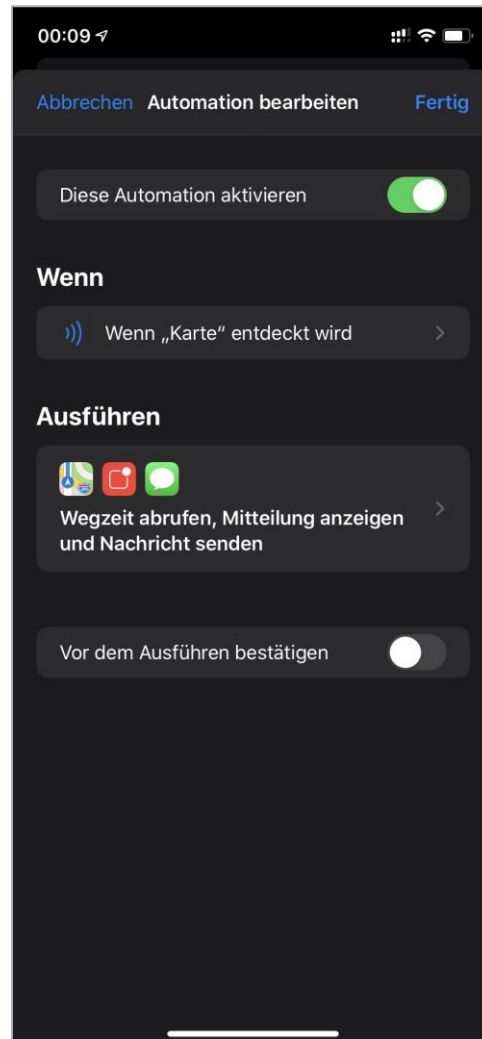
- Viele aktuelle Smartphones haben RFID Hardware eingebaut.
- Mit den passenden Apps können Tags gelesen und auch geschrieben werden.
- z.B. NFC Tag Reader / Writer von NXP <https://bit.ly/35lxKsV>
- NFC Tools von wakdev <https://bit.ly/2MXObJ8>
- Je nach Gerät unterschiedliche Hardware- und Software-Unterstützung.
- iOS seit Version 11, seit 13 auch Schreiben. iPhone  $\geq$  6(S)
  - › Shortcuts App
- Kann zur Automatisierung von Funktionen genutzt werden.



# ›Howto: Tags mit dem Smartphone auslesen



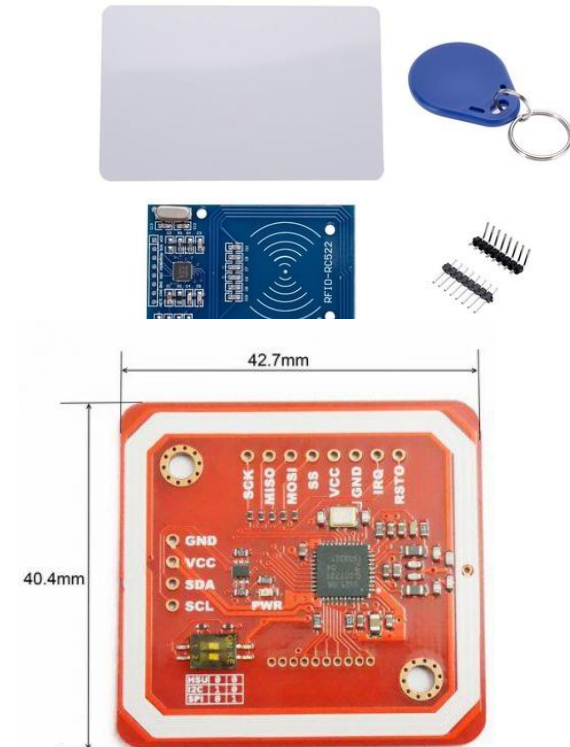
## ›Howto: Automation



# RFID Hardware für Maker

## ›RFID Hardware für Maker (13,56 MHz)

- MFRC522
  - › SPI (UART + I2C) Interface
  - › Gute Softwareunterstützung
  - › <https://bit.ly/1EpmmAk>
  - › Sehr günstig (ab 3 €)
- PN532
  - › SPI oder I2C Interface
  - › Ebenfalls sehr gute Bibliotheken von Seed-Studio und Adafruit
  - › Sehr günstig (ab 5 €)
- Karten / Tags
  - › Mifare Classic 1k/4K
  - › NTAG 213 (180 Bytes), 215 (540 Bytes), 216 (924 Bytes)
  - › Mifare Ultralight (schlechtere Unterstützung in Bibliotheken)

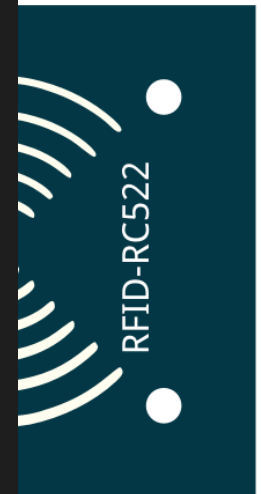


# RFID im eigenen Projekt

## ›RFID im eigenen Projekt: Arduino



```
1  #include <SPI.h>      // Import SPI-Bibliothek
2  #include <MFRC522.h>  // Import RFID-Bibliothek
3
4  MFRC522 rfidReader(53, 9); // Uno => Pin 10 / 9
5
6  void setup()
7  {
8      Serial.begin(9600); // Serielle Verbindung
9      SPI.begin();        // SPI-Verbindung aufbauen
10     rfidReader.PCD_Init(); // RFID-Reader initial.
11 }
12
13 void loop()
14 {
15     // Karte erkannt und gelesen
16     if (rfidReader.PICC_IsNewCardPresent() && rfidReader.PICC_ReadCardSerial()) {
17         Serial.print("RFID-TAG => ");
18
19         // Bytes der ID lesen und ausgeben
20         Serial.print("-");
21         for (byte i = 0; i < rfidReader.uid.size; i++) {
22             Serial.print(rfidReader.uid.uidByte[i], HEX);
23             Serial.print("-");
24         }
25         Serial.println(); // Ausgabe: RFID-TAG => -14-A3-F2-48-
26     }
27 }
```



## ›RFID im eigenen Projekt: Raspberry Pi

```
1  from time import sleep
2  import sys
3  from mfrc522 import SimpleMFRC522
4  reader = SimpleMFRC522()
5
6  try:
7      while True:
8          print("Hold a tag near the reader")
9          id, text = reader.read()
10         print("ID: %s\nText: %s" % (id,text))
11         sleep(5)
12 except KeyboardInterrupt:
13     GPIO.cleanup()
14     raise
```

$\pi$

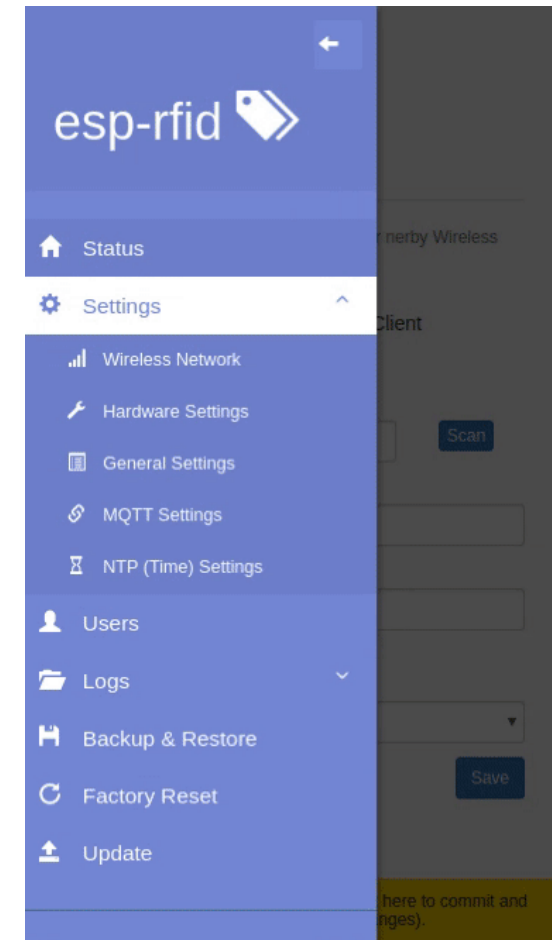
Demo



# Projektbeispiele

# Projektbeispiel: ESP RFID

- › Access Control System (ACS) mit Unterstützung für versch. günstige Reader (MFRC522, PN532 RFID, RDM6300).
- › Nutzt den ESP 8266 als Controller und bietet darüber ein Webinterface.
- › MQTT Unterstützung
- › <https://github.com/esprfid/esp-rfid>
- › Bietet keine wirkliche Sicherheit, da nur die UUID geprüft wird.
- › Loggt alle Zugriffe



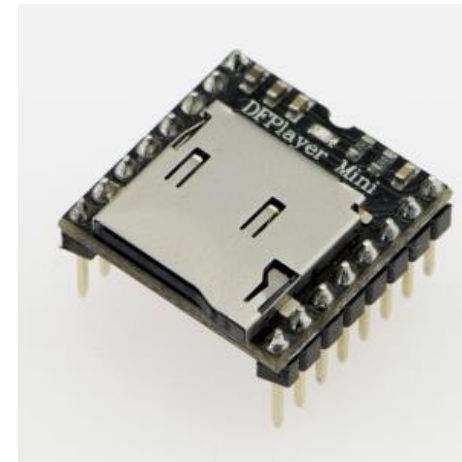
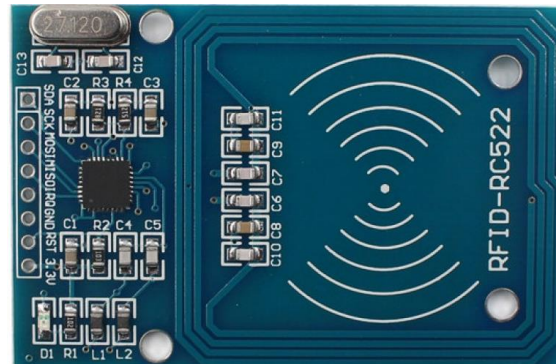
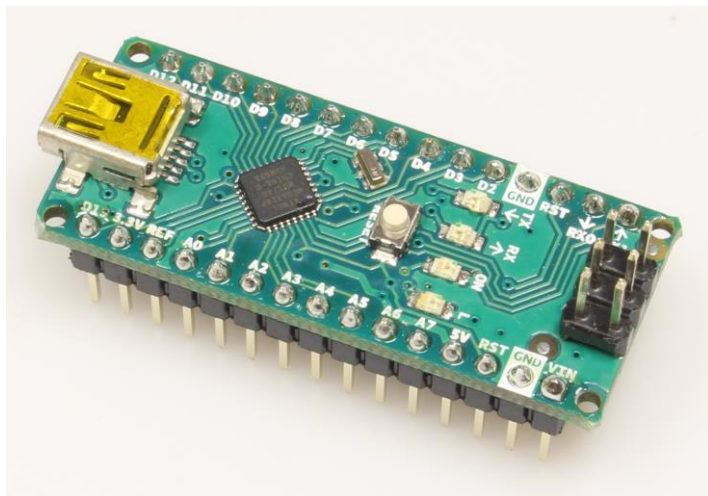
# Projektbeispiel: MP3-Player mit RFID Steuerung

- › Tonuino Projekt: <https://github.com/xfjx/TonUINO>
- › Bis zu 100 Alben auf SD-Karte durch Auflegen einer RFID-Karte aufrufbar.
- › 3-Knopf-Bedienung
- › Sehr günstige Hardware und leicht zu bauen.
- › Sparsam → Batteriebetrieb möglich

# Projektbeispiel: MP3-Player mit RFID Steuerung



# Projektbeispiel: MP3-Player mit RFID Steuerung



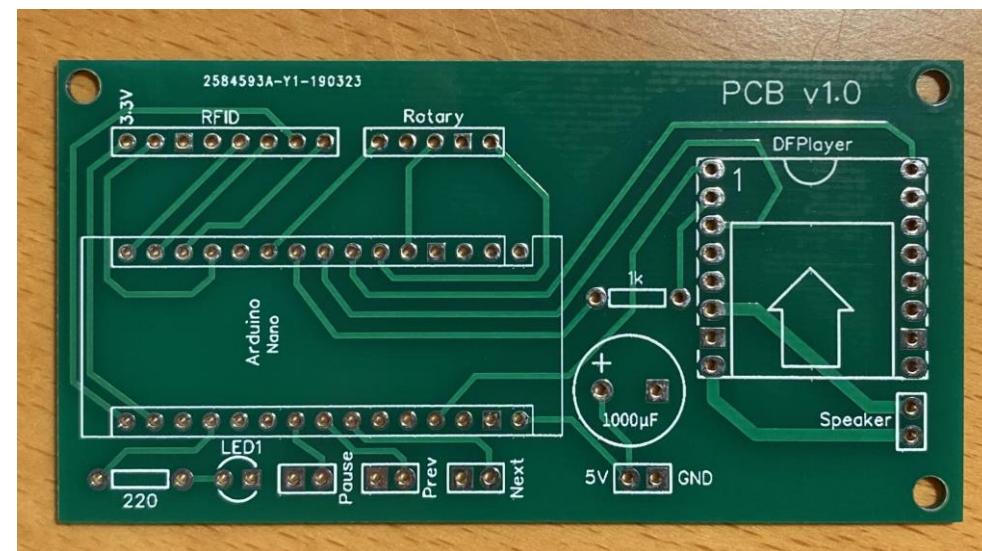
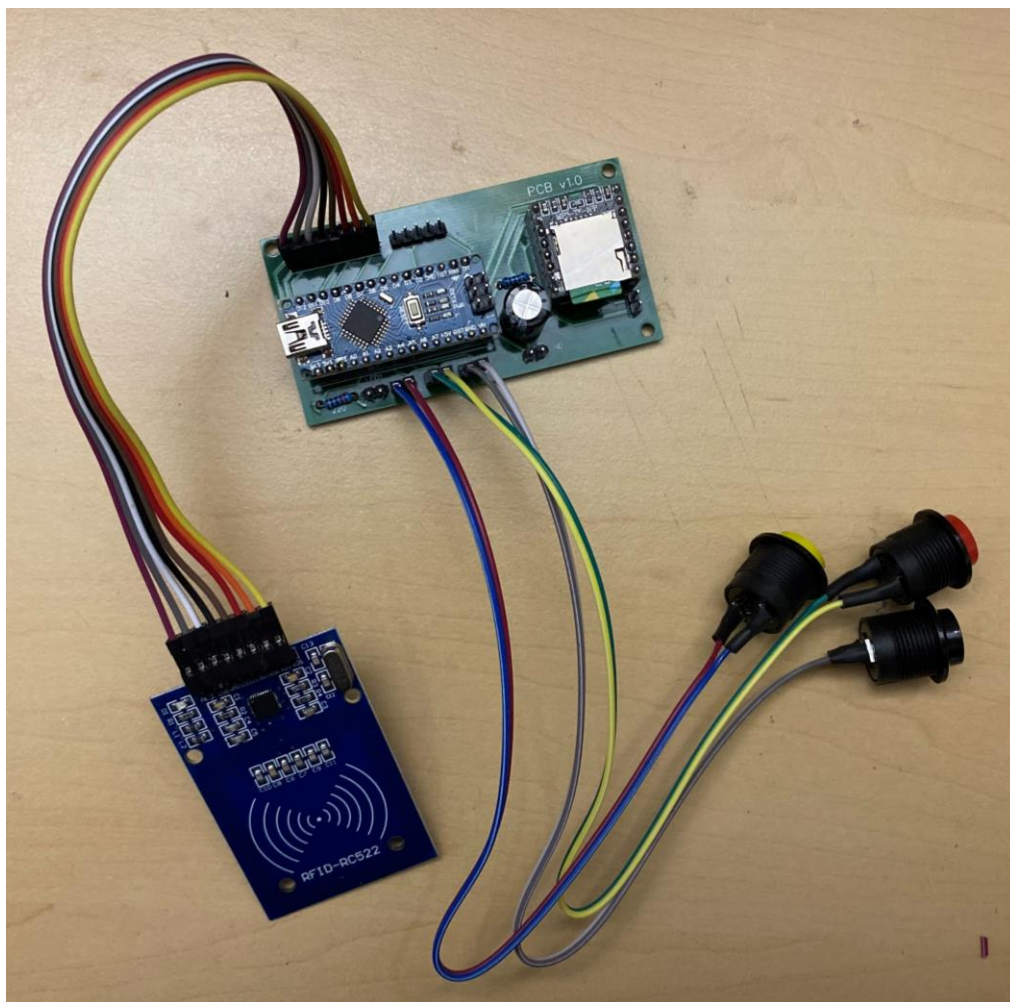
# Projektbeispiel: MP3-Player mit RFID Steuerung

## › Teileliste:

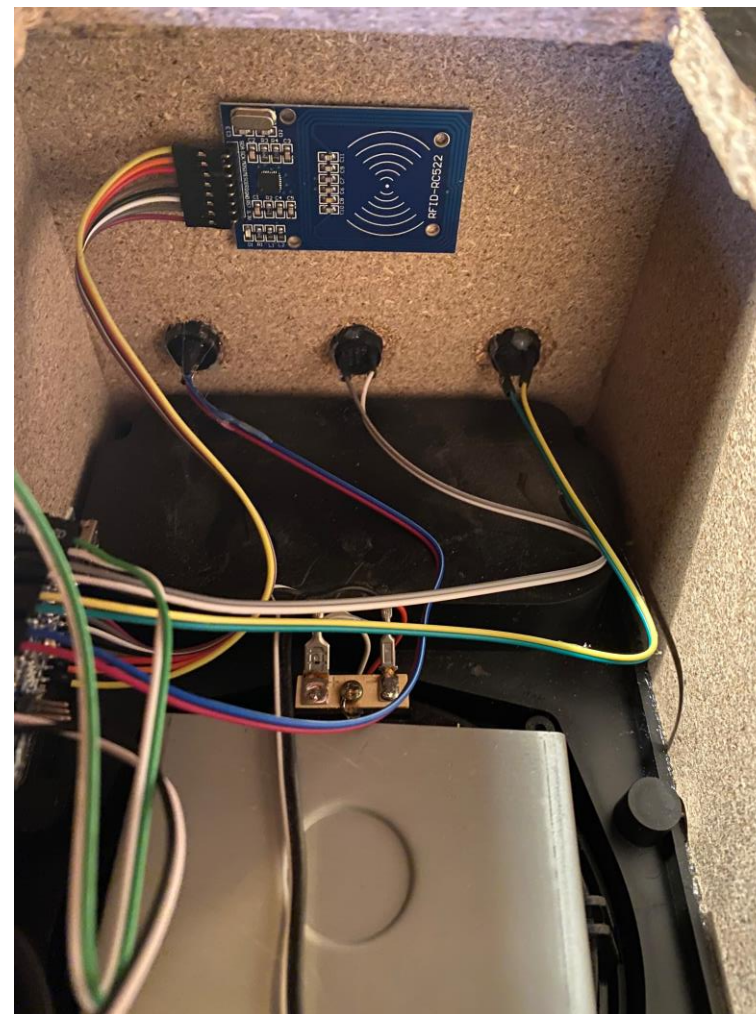
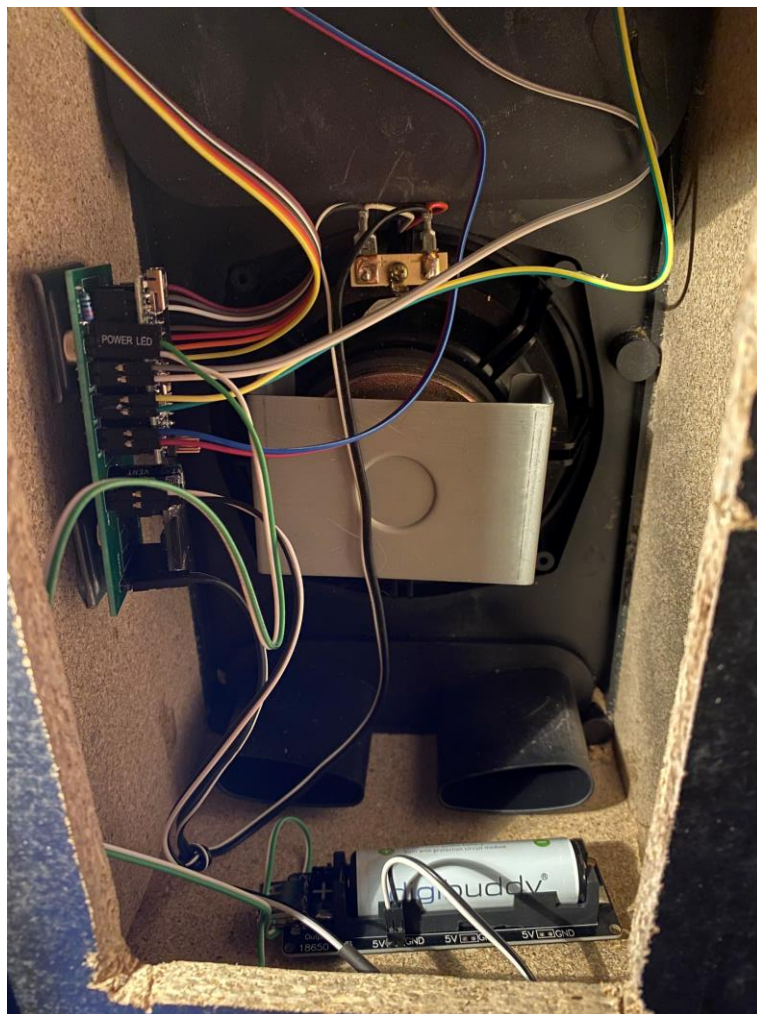
- MFRC522 RFID Reader, ab 2,50 €
- Arduino Nano (ATmega328P), ab 3,00 €
- DF Player Mini, ab 2,00 €
- Pushbutton, Ein-/Ausschalter
- USB Powerbank oder USB Netzteil
- Lautsprecher
- RFID Karten Mifare Classic, < 0,50 € pro Stück



# Projektbeispiel: MP3-Player mit RFID Steuerung



# Projektbeispiel: MP3-Player mit RFID Steuerung





# Projektbeispiel: MP3-Player mit RFID Steuerung



# Projektbeispiel: MP3-Player mit RFID Steuerung



# Vielen Dank!

- › Feedback und Fragen gerne per E-Mail:  
[pi@tobiasblum.de](mailto:pi@tobiasblum.de)